LAWTRUST CERTIFICATE POLICY

Law Trusted Third Party Services (Pty) Ltd

Registration number 2001/004386/07

("LAWtrust")

20 Woodlands Drive,

Woodlands Office Park, Woodmead,

Johannesburg, South Africa

Phone +27 (0)12 676 9240 • Fax +27 (0)12 665 3997

Web https://www.lawtrust.co.za • eMail governance@lawtrust.co.za

LAWtrust reserves the right to change or amend this certification practice statement at any time without prior notice. Changes will be posted on the LAWtrust website [https://www.lawtrust.co.za/repository] from time to time. If you have any queries about this document, please contact LAWtrust.

DOCUMENT CONTROL

Document history

Version Number	Effective Date	Author	Summary of Changes	Status
V01 13-02-2007	13-02-2007	B Anderson	Review	Expired
V02 17-05-2010	17-05-2010	N van Greunen	Review	Expired
V03 06-12-2013	06-13-2013	N van Greunen	Logo changes and Review	Expired
V04 05-12-2014	05-12-2014	N van Greunen	Review	Expired
V05 18-11-2015	01-12-2015	B Anderson	Review	Expired
V006 2016-12-21	2016-12-21	Bruce Anderson	Amended logo, Added approval Signature on last page, Updated Certificate profiles, deleted CA1 and added CA2	Expired
V023_2025_08_07	2017-02-21	B Anderson	Amendments as per Audit requirements	Expired
V008 2017-09-28	2017-10-01	B Anderson	Annual Review	Expired
V009 2018-06-15	2018-06-15	Bruce Anderson	Annual Review, amended (identity document definition, governing law, table overlap)	Expired
V010 2018-08-06	2018-08-06	B Anderson	Added Housekeeping items	Expired
V011 2018-12-14	2018-12-14	E Oosthuizen	Apply new document template, Address change	Expired
V012 2019-03-08	2019-03-08	E Oosthuizen	Review and Housekeeping items	Expired
V013 2020-02-13	2020-02-13	K Hlabathi	Annual review. Update AeSign CA01 certificate details after rekey	Expired

V014 2020-08-25	2020-08-25	M De Waal K Hlabathi	Updated with Root CA2 information	Expired
V015 2020-10-30	2020-11-25	K Hlabathi	Updated with new Issuing CA Profile information after the Key Ceremony	Expired
V016 2021-08-06	2021-08-06	M Masemene K Hlabathi	Updated the CP to conform to RFC3647 Standard	Expired
V016 2021-08-06	2021-08-18	K Hlabathi	Updated section 4.12, key escrow	Expired
V017 2022-10-24	2022-11-04	M De Waal	Yearly Update. Logo and Formatting changes	Expired
V018 2023-03-10	2023-03-10	M De Waal	Aligned retention periods with CPS's, addition of LT Secure CA01	Expired
V019 2023-07-12	2023-07-12	M De Waal	Addition of LT Auth CA02	Expired
V020 2023-09-01	2023-10-31	M De Waal	2023 Yearly update	Expired
V021 2024-09-02	2024-10-31	M De Waal	2024 Yearly review	Expired
V022 2025-03-27	2025-03-31	M De Waal	Updated max certificate lifetime to 3 years	Expired
V023 2025-08-07	2025-10-31	M De Waal	Yearly Update, removed LT2048CA2 references	Expired
V024 2026-08-07	2026-10-30	M De Waal	Yearly Update	Operational

Document references

References to the following documents have been made in the preparation of this document:

Ref.	Document Title	File Location
1	LAWtrust Certificate Policy	LAWtrust Internal Policy (Level 2)
2	LAWtrust Relying Party Agreement	https://www.lawtrust.co.za/repository
3	LAWtrust Subscriber Agreement	https://www.lawtrust.co.za/repository
4	LAWtrust Privacy Policy	https://www.altron.com/policies/privacy-policy/
5	LAWtrust mPKI Services Agreements	LAWtrust & Registration Authorities

Table of Contents

1. Introduction 12

1.1 Overview 13
1.1.1 Certificate Policy 13
1.1.2 Relationship between the CP and the CPS 13
1.1.3 Interaction with other PKIs 13
1.1.4 Scope 14

1.2 Document Name and Identification 14

1.3 PKI Participants 14
1.3.1 LAWtrust Public Key Infrastructure services (LAWtrust PKI) 15
1.3.2 LAWtrust Root CA 2048 16
1.3.3 LAWtrust Root CA (4096) 16
1.3.4 LAWtrust AeSign Certification Authority 2048 16
1.3.5 LAWtrust AeSign CA02 16
1.3.6 LAWtrust AATL CA01 16
1.3.7 LAWtrust Auth CA02 16
1.3.8 LAWtrust Signing CA01 17
1.3.9 LAWtrust Auth CA01 17
1.3.10 LAWtrust Secure CA01 17
1.3.11 LAWtrust Security Committee 17
1.3.12 Registration Authority (RA) 17
1.3.13 Subscribers 17
1.3.14 Relying Parties 18

1.4 Certificate Usage 18
1.4.1 Appropriate Certificate Uses 18
1.4.2 Prohibited Certificate Uses 19

1.5 Policy Administration 19
1.5.1 Administration Organization 19
1.5.2 Contact Person 19
1.5.3 Person Determining CPS Suitability for the Policy 19
1.5.4 CP Approval 19

1.6 Definitions and Acronyms 20

2. Publication and Repository Responsibilities 20

2.1 Repositories 20

2.2 Publication of Certification Information 20
2.2.1 Publication of Certificates and Certificate Status 20
2.2.2 Publication of CA Information 20
2.2.3 Interoperability 21

2.3 Time or Frequency of Publication 21

2.4 Access Controls on Repositories 21

3. Identification and Authentication 21

3.1 Naming 21
3.1.1 Types of Names 21
3.1.2 Need for Names to be Meaningful 22
3.1.3 Anonymity or Pseudonymity of Subscribers 22
3.1.4 Rules for Interpreting Various Name Forms 22
3.1.5 Uniqueness of Names 22
3.1.6 Recognition, Authentication, and Role of Trademarks 22

3.2 Initial Identity Validation 23
3.2.1 Method to Prove Possession of Private Key 23
3.2.2 Authentication of organizational entity 23
3.2.3 Non-verified Subscriber Information 24
3.2.4 Validation of Authority 24
3.2.5 Criteria of Interoperation 24

3.3 Identification and Authentication for Re-key Requests 24
3.3.1 Identification and Authentication for Routine Re-Key 24
3.3.2 Identification and Authentication for Re-key After Revocation 24

3.4 Identification and Authentication for Revocation Requests 25

4. Certificate Life-Cycle Operational Requirements 25

4.1 Certificate Application 25
4.1.1 Submission of Certificate Application 25
4.1.2 Enrollment Process and Responsibilities 26

4.2 Certificate Application Processing 26
4.2.1 Performing Identity-proofing Functions 26
4.2.2 Approval or Rejection of Certificate Applications 26
4.2.3 Time to Process Certificate Applications 27

4.3 Certificate Issuance 27
4.3.1 CA Actions During Certificate Issuance 27
4.3.2 Notification of Certificate Issuance 28

4.4 Certificate Acceptance 28
4.4.1 Conduct Constituting Certificate Acceptance 28
4.4.2 Publication of the Certificate by the CA 28
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 28

4.5 Key Pair and Certificate Usage 28
4.5.1 Private Key and Certificate Usage 28
4.5.2 Relying Party Public Key and Certificate Usage 29

4.6 Certificate Renewal 29
4.6.1 Circumstances for Certificate Renewal 29
4.6.2 Who may request Certificate Renewal 29
4.6.3 Processing Certificate Renewal Requests 30
4.6.4 Notification of Renewed Certificate Issuance 30
4.6.5 Conduct constituting acceptance of a renewal certificate 30

4.6.6 Publication of a Renewal Certificate 30
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 30

4.7 Certificate Re-Key 30
4.7.1 Circumstances for Certificate Re-key 30
4.7.2 Who can Request a Certificate Re-key 31
4.7.3 Processing Certificate Re-keying Requests 31
4.7.4 Notification of a Re-keyed Certificate Issuance 31
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 31
4.7.6 Publication of the Re-keyed Certificate by the CA 31
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 31

4.8 Certificate Modification 32

4.9 Certificate Revocation and Suspension 32
4.9.1 Circumstance for Revocation of a Certificate 32
4.9.2 Who Can Request Revocation of a Certificate 33
4.9.3 Procedure for Revocation Request 34
4.9.4 Revocation Request Grace Period 34
4.9.5 Time within which CA must Process the Revocation Request 34
4.9.6 Revocation Checking Requirements for Relying Parties 34
4.9.7 CRL Issuance Frequency 34
4.9.8 Maximum Latency of CRLs 34
4.9.9 Online Revocation Checking Availability 34
4.9.10 Online Revocation Checking Requirements 35
4.9.11 Other Forms of Revocation Advertisements Available 35
4.9.12 Special Requirements Related To Key Compromise 35
4.9.13 Circumstances for Certificate Suspension 35
4.9.14 Who Can Request Suspension 35
4.9.15 Procedure for Suspension Request 36
4.9.16 Limits on Suspension Period 36
4.9.17 Circumstances for Terminating Suspended Certificates 36
4.9.18 Procedure for Terminating the Suspension of a Certificate 36

4.10 Certificate Status Services 37

4.11 End of Subscription 37

4.12 Key Escrow and Recovery 37

5. Facility Management and Operational Controls 37

5.1 Physical Security Controls 37
5.1.1 Site Location and Construction 37
5.1.2 Physical Access 38
5.1.3 Power and Air Conditioning 38
5.1.4 Water Exposure 38
5.1.5 Fire Prevention and Protection 38
5.1.6 Media Storage 39
5.1.7 Waste Disposal 39
5.1.8 Off-Site Backup 39

5.2 Procedural Controls 39
5.2.1 Trusted Roles 39
5.2.2 Number of Persons Required per Task 40
5.2.3 Identification and Authentication for Each Role 40
5.2.4 Separation of Roles 40

5.3 Personnel Controls 40
5.3.1 Qualifications, Experience And Clearance Requirements 40
5.3.2 Background Check and Clearance Procedures 40
5.3.3 Training Requirements 41
5.3.4 Retraining Frequency and Requirements 41
5.3.5 Job Rotation Frequency and Sequence 41
5.3.6 Sanctions for Unauthorized Actions 41
5.3.7 Contracting Personnel Requirements 41
5.3.8 Documentation Supplied to Personnel 42

5.4 Audit Logging Procedures 42
5.4.1 Types of Events Recorded 42
5.4.2 Frequency of Processing Data 43
5.4.3 Retention Period for Audit Log 44
5.4.4 Protection of Audit Log 44
5.4.5 Audit Log Backup Procedures 44
5.4.6 Audit Collection System (Internal or External) 44
5.4.7 Notification to Event-Causing Subject 44
5.4.8 Vulnerability Assessments 44

5.5 Records Archival 45
5.5.1 Types of Events Archived 45
5.5.2 Retention Period for Archive 45
5.5.3 Protection of Archive 45
5.5.4 Archive Backup Procedures 45
5.5.5 Requirements for Time-Stamping of Records 45
5.5.6 Archive Collection System 45
5.5.7 Procedures to Obtain and Verify Archive Information 46

5.6 Key Changeover 46

5.7 Compromise and Disaster Recovery 46
5.7.1 Incident and Compromise Handling Procedures 46
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 46
5.7.3 CA Private Key Compromise Recovery Procedures 46
5.7.4 Business Continuity Capabilities after a Disaster 46

5.8 CA OR RA Termination 47
5.8.1 CA Termination 47
5.8.2 RA Termination 47

6. Technical Security Controls 48

6.1 Key Pair Generation and Installation 48
6.1.1 Key Pair Generation 48
6.1.2 Private Key Delivery to Subscribers 48

6.1.3 Public Key Delivery to Certificate Issuer 49
6.1.4 CA Public Key Delivery to Relying Parties 49
6.1.5 Key Sizes 49
6.1.6 Public Key Parameters Generation and Quality Checking 50
6.1.7 Key Usage Purposes 50

6.2 Private Key Protection and Crypto-Module Engineering Controls 50
6.2.1 Cryptographic Module Standards and Controls 50
6.2.2 CA Private Key Multi-Person Control 50
6.2.3 Private Key Escrow 50
6.2.4 Private Key Backup 51
6.2.5 Private Key Archival 51
6.2.6 Private Key Transfer Into or From a Cryptographic Module 51
6.2.7 Private Key Storage on Cryptographic Module 51
6.2.8 Method of Activating Private Keys 51
6.2.9 Methods of Deactivating Private Keys 52
6.2.10 Methods of Destroying Private Keys 52
6.2.11 Cryptographic Module Rating 52

6.3 Other Aspects of Key Pair Management 52
6.3.1 Public Key Archive 52
6.3.2 Certificate Operational Periods and Key Usage Periods 52

6.4 Activation Data 53
6.4.1 Activation Data Generation and Installation 53
6.4.2 Activation Data Protection 53
6.4.3 Other Aspects of Activation Data 54

6.5 Computer Security Controls 54
6.5.1 Specific Computer Security Technical Requirements 54
6.5.2 Computer Security Rating 54

6.6 Life-Cycle Security Controls 54
6.6.1 System Development Controls 54
6.6.2 Security Management Controls 54
6.6.3 Life Cycle Security Ratings 55

6.7 Network Security Controls 55

6.8 Time Stamping 55

7. Certificate, CRL and OCSP Profiles 55

7.1 Certificate Profile 55
7.1.1 Version Numbers 55
7.1.2 Certificate Extensions 55
7.1.3 Algorithm Object Identifiers 56
7.1.4 Name Forms 56
7.1.5 Name Constraints 56
7.1.6 Certificate Policy Object Identifier 56
7.1.7 Usage of Policy Constraints Extension 56
7.1.8 Policy Qualifiers Syntax and Semantics 56

7.1.9 Processing Semantics for the Critical Certificate Policy Extension 56

7.2 CRL Profile 56

7.2.1 Version Numbers 57

7.2.2 CRL and CRL Entry Extensions 57

7.3 OCSP Profile 57

7.3.1 Version Number 58

7.3.2 OCSP Extensions 58

8. Compliance Audit and Other Assessments 58

8.1 Frequency of Audit or Assessments 58

8.2 Identity and Qualifications of Assessor 58

8.3 Assessor's Relationship to Assessed Entity 59

8.4 Topics Covered By Assessment 59

8.5 Actions Taken As A Result of Deficiency 59

8.6 Communication of Results 59

9. Other Business and Legal Matters 60

9.1 Fees 60

9.1.1 Certificate Issuance/Renewal Fee 60

9.1.2 Certificate Access Fees 60

9.1.3 Revocation or Status Information Access Fee 60

9.1.4 Fees for Other Services 60

9.1.5 Refund Policy 60

9.2 Financial Responsibility 60

9.2.1 Insurance Coverage 60

9.2.2 Other Assets 61

9.2.3 Insurance/warranty Coverage for End-Entities 61

9.3 Confidentiality of Business Information 61

9.3.1 Scope of Confidential Information 61

9.3.2 Information not within the Scope of Confidential Information 61

9.3.3 Responsibility to Protect Confidential Information 61

9.4 Privacy of Personal Information 61

9.4.1 Privacy Plan 62

9.4.2 Information Treated as Private 62

9.4.3 Information not Deemed Private 62

9.4.4 Responsibility to Protect Private Information 62

9.4.5 Notice and Consent to Use Private Information 62

9.4.6 Disclosure Pursuant to Judicial/Administrative Process 62

9.4.7 Other Information Disclosure Circumstances 62

9.5 Intellectual Property Rights 62

9.6 Representations and Warranties 63

9.6.1 LAWtrust PKI CA's Representations and Warranties 63
9.6.2 RA Representations and Warranties 64
9.6.3 Relying Parties Representations and Warranties 64
9.6.4 Subscriber Representations and Warranties 64
9.7 Disclaimers of Warranties 65
9.8 Limitations of Liability 65
9.9 Indemnities 66
9.10 Term and Termination 66
9.10.1 Term 66
9.10.2 Termination 67
9.10.3 Effect of Termination and Survival 67
9.11 Individual Notices and Communications with Participants 67
9.12 Amendments 67
9.12.1 Procedure for Amendment 67
9.12.2 Notification Mechanism and Period 67
9.12.3 Circumstances under which OID must be changed 68
9.13 Dispute Resolution Procedures 68
9.14 Governing Law 68
9.15 Compliance with Applicable Law 68
9.16 Miscellaneous Provisions 68
9.16.1 Entire Agreement 68
9.16.2 Assignment 68
9.16.3 Severability 68
9.16.4 Enforcement (Attorney Fees/Waiver of Rights) 69
9.16.5 Force Majeure 69
9.17 Other Provisions 69
9.17.1 Fiduciary Relationships 69
9.17.2 Administrative Processes 69
10. Appendix A (Definitions) 70
11. Sign Off Acceptance 75

1. INTRODUCTION

Law Trusted Third Party Services (Pty) Ltd ("LAWtrust") [https://www.lawtrust.co.za] conducts the business of providing trusted third-party authentication and public key cryptography services.

LAWtrust manages and operates a PKI hierarchy offering certification services from the LAWtrust managed issuing CA's to their clients. The LAWtrust Hierarchy consists of two Root CAs and all issuing CA's signed into those Root CAs

These services include:

1. appointing third party customer Registration Authorities ("RA"),
2. training and monitoring certificate administrators appointed by RA(s),
3. the issuing of digital certificates by the certificate authorities it operates,
4. managing the lifecycle of digital certificates issued,
5. providing reference information on the status of all digital certificates issued.

Digital certificates, containing a public key, identify the person who is the holder of the associated private key used to digitally sign an electronic transaction. This forms the basis of positive identity, message integrity, and non-repudiation when conducting business electronically. Private keys may also be used to achieve confidentiality.

This LAWtrust Certificate Policy introduces the rules that LAWtrust requires adherence to, in order to ensure a high level of trust in the digital certificates issued by the LAWtrust CA(s). Digital certificates, properly issued, are an effective risk management tool used to address the business need for positive identity, privacy and non-repudiation.

In order to address the above-mentioned requirements and goals, LAWtrust operates the following publicly trusted CAs:

- LAWtrust Root CA 2048
- LAWtrust Root CA2 (4096)
- LAWtrust AATL CA01
- LAWtrust AeSign Certification Authority 2048
- LAWtrust AeSign CA02
- LAWtrust Auth CA02
- LAWtrust Auth CA01
- LAWtrust Signing CA01
- LAWtrust Secure CA01

This LAWtrust CP shall define the policies by which the LAWtrust CAs operates. This CP complies with the format of the Internet Request for Comment (RFC) 3647 [RFC 3647].

1.1 Overview

This CP defines a high level of trust and assurance for use by all LAWtrust CAs participants.

The LAWtrust Root CA 2048 and LAWtrust Root CA 4096 are offline Root CAs that will issue certificates to approved Level 2 Issuing CAs. Different Subscriber type certificates based on the business requirement will be issued from the level 2 subordinate Issuing CAs.

This CP has been developed under the direction of the LAWtrust Policy Authority (PA) who has the responsibility for directing the development, seek approval and update of this LAWtrust CP.

Any use of or reference to this CP outside the context of the LAWtrust PKI is completely at the using party's risk.

It is the responsibility of all parties applying for or using a Digital Certificate issued under this CP, to read this CP and understand the practices established for the lifecycle management of the Certificates issued by the LAWtrust CAs. Any application for Digital Certificates or reliance on validation services of the LAWtrust CA issued Certificates signifies understanding and acceptance of this CP and its supporting policy documents.

1.1.1 Certificate Policy

X.509 certificates issued by the LAWtrust CAs will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a certificate is trusted for a particular purpose.

1.1.2 Relationship between the CP and the CPS

The LAWtrust CP states what assurance can be placed in a certificate issued by LAWtrust CAs. The Certificate Practice Statement (CPS) states how LAWtrust PKI meets the requirements of this CP.

The CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by LAWtrust CAs as governed by this CP and related documents which describe the LAWtrust PKI requirements and use of Certificates.

1.1.3 Interaction with other PKIs

No Stipulation.

1.1.4 Scope

This CP applies to all certificates issued by LAWtrust CAs. The LAWtrust CAs operate under the LAWtrust PKI hierarchy, maintained and operated by LAWtrust for issuance and management of certificates and revocation lists under the hierarchy. More specifically, the LAWtrust PKI consists of offline CAs (LAWtrust Root CA 2048 and LAWtrust Root CA 4096), which issue certificates to approved sub-CAs, who in turn will issue subscriber certificates.

The management of the resources required to operate the LAWtrust CA(s) is in accordance with the provisions contained in the respective LAWtrust Certification Practice Statements ("LAWtrust CPS(s)") of the CAs.

These resources include registration authorities, personnel, network infrastructure, IT systems, cryptographic material, physical locales, and information assets.

1.2 Document Name and Identification

This document is the LAWtrust Certificate Policy (CP), and is identified by the object identifier (OID):

OID: 1.3.6.1.4.1.54383.1

1.3 PKI Participants

The following are subcomponents of LAWtrust CAs that are governed by this CP.

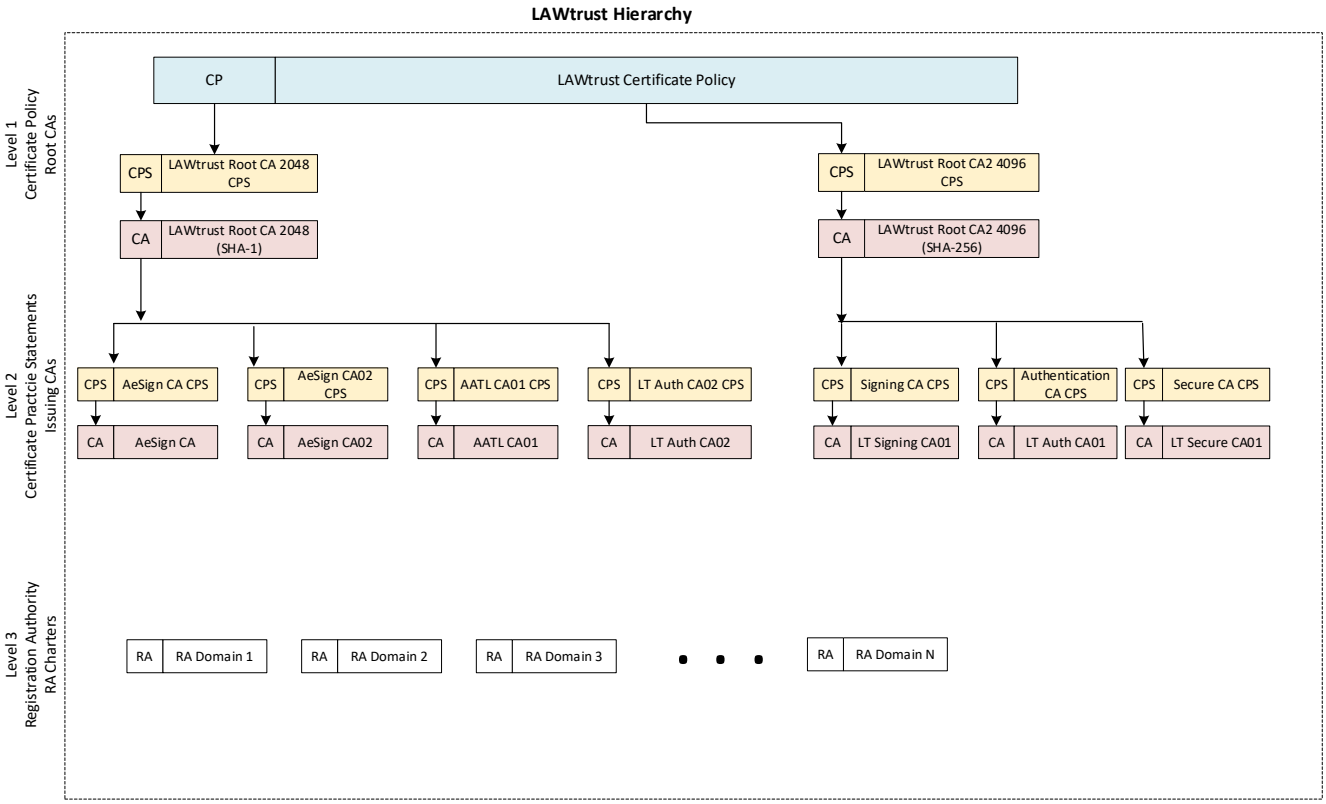


Figure 1. LAWtrust PKI Hierarchy

1.3.1 LAWtrust Public Key Infrastructure services (LAWtrust PKI)

The LAWtrust PKI is an umbrella term referring to LAWtrust (a division of Altron TMT Pty Ltd) as an organization that runs PKI services under the two LAWtrust Roots, the LAWtrust Root CA 2048 and LAWtrust Root CA (4096). The hierarchy managed by LAWtrust is shown in the diagram above. This Certificate Policy provides the policy statements for the hierarchy within the LAWtrust PKI. Each Root CA has a dedicated CPS and each Issuing CA chained into the Root CAs has their own dedicated CPS.

The Issuing CAs will issue subscriber certificates, OCSP responder certificates and other certificates required by PKI components. The Issuing CAs will issue certificates to Subscribers in accordance with this CP and corresponding CPS, any RA Agreement, Subscriber Agreement, Relying Party Agreement, and the LAWtrust PKI Policy.

LAWtrust as an entity is responsible for:

- Control over the designation of CAs and RAs;
- Conduct regular internal security audits;

- Performance of all aspects of the services, operations and infrastructure related to the LAWtrust PKI.

1.3.2 LAWtrust Root CA 2048

The LAWtrust Root CA is a self-signed Root-CA. It issues certificates to the LAWtrust Issuing CAs underneath the PKI hierarchy.

1.3.3 LAWtrust Root CA (4096)

The LAWtrust Root CA 4096 is a self-signed Root-CA. It issues certificates to the LAWtrust Issuing CAs underneath the PKI hierarchy.

1.3.4 LAWtrust AeSign Certification Authority 2048

The LAWtrust AeSign Certification Authority 2048 Issuing CA is an issuing Certificate Authority under the LAWtrust Root CA 2048. The CA issues accredited digital certificates compliant with the stipulations of the ECT Act (Act 68 of 2002) to user individuals and organization entities. It digitally signs, issues and revokes certificates for digital signature certificates.

1.3.5 LAWtrust AeSign CA02

The LAWtrust AeSign CA2 Issuing CA is an issuing Certificate Authority under the LAWtrust Root CA 2048. The CA issues accredited digital certificates compliant with the stipulations of the ECT Act (Act 68 of 2002) to user individuals and organization entities. It digitally signs, issues and revokes certificates for digital signature certificates.

1.3.6 LAWtrust AATL CA01

The LAWtrust AATL CA01 Issuing CA is an issuing Certificate Authority under the LAWtrust Root CA 2048. It issues different types of certificates to user individuals and organization entities. It digitally signs, issues, revokes certificates for digital signature certificates that are in compliant with the requirements of the Adobe Approved Trust List (AATL) program.

1.3.7 LAWtrust Auth CA02

The LAWtrust Auth CA01 Issuing CA is an issuing Certificate Authority under the LAWtrust Root CA 2048. It issues different types of certificates to user individuals, their computers, organization roles, devices, and applications. It digitally signs, issues and revoke digital signature certificates mainly used for authentication purposes.

1.3.8 LAWtrust Signing CA01

The LAWtrust Signing CA01 Issuing CA is an issuing Certificate Authority under the LAWtrust Root CA2 (4096). It issues different types of certificates to user individuals and organization entities. It digitally signs, issues and revoke certificates as part of the digital signature certificate services. This CA is also in compliant with the provisions of the Adobe Approved Trust List program. It also issues digital certificates that are accredited under the ECT Act.

1.3.9 LAWtrust Auth CA01

The LAWtrust Auth CA01 Issuing CA is an issuing Certificate Authority under the LAWtrust Root CA2 (4096). It issues different types of certificates to LAWtrust user individuals, their computers, organization roles, devices, and applications. It digitally signs, issues and revoke digital signature certificates mainly used for authentication purposes.

1.3.10 LAWtrust Secure CA01

The LAWtrust Secure CA01 Issuing CA is an issuing Certificate Authority under the LAWtrust Root CA2 (4096). It issues different types of certificates to LAWtrust user individuals, their computers, organization roles, devices, and applications. It digitally signs, issues and revoke digital signature certificates mainly used for secure email.

1.3.11 LAWtrust Security Committee

The LAWtrust Security committee is responsible for the approval of PKI Policies and overseeing the security operations of the LAWtrust PKI.

1.3.12 Registration Authority (RA)

LAWtrust PKI may delegate the identification of subscribers and any other related functions to other entities. These entities act on behalf of LAWtrust PKI for the purpose of collecting subscriber information and identity.

1.3.13 Subscribers

Subscribers are end users that are issued with the certificates from the Level-2 Issuing CAs. The subscribers can be human beings, legal entities or devices (servers, network devices, communication equipment, etc.).

Subscribers are bound by the conditions of use of certificates as contained in the Subscriber Agreement. In general, the subscribers assert that they use the key and certificate in accordance with this CP and applicable CPS.

1.3.14 Relying Parties

A Relying Party in this context is the entity that relies on the validity of the binding of the LAWtrust Root CA 2048, LAWtrust Root CA2 (4096) (and signed Issuing CAs) identity to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by LAWtrust CAs. A Relying Party's right to rely on a certificate issued under this CP, requirements for reliance, and limitations thereon, are governed by the terms of the LAWtrust CP and the Relying Party Agreement.

Relying Parties shall use the LAWtrust PKI, and rely on a certificate that has been issued under the LAWtrust CP if:

- The certificate has been used for the purpose for which it has been issued, as described in the LAWtrust CP;
- The Relying Party has verified the validity of the digital certificate, using procedures described in the Relying Party Agreement;
- The Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate; and
- The relying party accepts in totality, the certificate policy applicable to the certificate, which can be identified by reference of the certificate policy OID mentioned in the certificate.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

LAWtrust Root CA 2048 only issues Sub-CA certificates for the issuing certificate authorities that are part of the PKI hierarchy. In particular, it issues certificates to the LAWtrust AeSign Certification Authority 2048, LAWtrust AeSign CA02, LAWtrust AATL CA01, and LAWtrust Auth CA02.

LAWtrust Root CA2 (4096) only issues Sub-CA certificates for the issuing certificate authorities that are part of the PKI hierarchy. It issues certificates to the LAWtrust Signing CA01, LAWtrust Auth CA01 and Lawtrust Secure CA01.

The LAWtrust Issuing CAs issue Subscriber (including devices) and Online Certificate Status Protocol (OCSP) responder certificates. The subscriber certificates are used for multiple purposes, depending on the Key Usage extensions set. OCSP Responder certificates are used to sign responses for certificate status information requests.

The LAWtrust Issuing CAs issue certificates under this CP only to those Subscribers who have signed their acceptance of a Subscriber Agreement, or in the case of devices, those devices

that have been properly identified as belonging to LAWtrust, or if belonging to outside entities, they have been identified as requiring such certificates.

1.4.2 Prohibited Certificate Uses

Certificates issued under this CP shall not be authorized for use in any circumstances or in any application which is illegal under South African law, could lead to death, personal injury or damage to property, or in conjunction with on-line control equipment in hazardous environments such as in the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control or direct life support machines, and the LAWtrust CAs shall not be liable for any claims arising from such use.

1.5 Policy Administration

1.5.1 Administration Organization

This CP is administered by the LAWtrust PA and approved by the LAWtrust Security Committee. The LAWtrust PA signs-off on the approved PKI Policy documents.

1.5.2 Contact Person

Queries regarding the LAWtrust CP shall be directed to:

Email: governance@lawtrust.co.za

Telephone: +27126769240

Any formal notices required by this CP shall be sent in accordance with the notification procedures specified in section 9.12.2 of this CP.

1.5.3 Person Determining CPS Suitability for the Policy

The LAWtrust PA is responsible for ensuring that all LAWtrust CPS documents conform to the requirements of this CP in accordance with policies and procedures specified by LAWtrust. The PA shall ensure that the CPS, after ensuring conformity to the CP, is approved by the LAWtrust Security Committee.

1.5.4 CP Approval

Changes or updates to this LAWtrust CP document must be made in accordance with the provisions contained in this CP and are subject to LAWtrust Security Committee approval. The approved changes shall be published at the LAWtrust PKI repository located at https://www.lawtrust.co.za/repository

1.6 Definitions and Acronyms

The terms used in this document shall have the meanings as defined in **Appendix A** of this document.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

LAWtrust PKI shall maintain repositories in the form of directories and/or URL locations where issued certificates and certificate status information (e.g. CRLs) will be published.

The repositories shall provide access through an appropriate standard-based access control. The repositories shall be made available on a 24/7 basis and designed in such a way as to maintain high availability throughout operations.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

LAWtrust Root CA(s) shall publish in the appropriate repository: CA Certificates and CRLs.

LAWtrust Issuing CA(s) shall publish CA Certificates, subscriber certificates and CRLs in the appropriate repository.

Issuing CAs that make use of the Online Certificates Status Protocol (OCSP) shall publish the status of the certificate at the location specified in the certificate.

The LAWtrust PA will decide on directory access restrictions to prevent misuse and unauthorized harvesting of information.

2.2.2 Publication of CA Information

This CP shall be available to all LAWtrust PKI participants at the LAWtrust website, https://www.lawtrust.co.za/repository. This website is the only source for up-to-date documentation and LAWtrust PKI reserves the right to publish newer versions of the documentation without prior notice.

Additionally, LAWtrust will publish an approved, current, and digitally signed version of LAWtrust Certificate Practice Statement (CPS) for all the CAs under the LAWtrust PKI Hierarchy.

LAWtrust Public LDAP directory and LAWtrust website (https://www.lawtrust.co.za/repository) are the only authoritative sources for:

- All publicly accessible certificates of the LAWtrust CAs;

2.2.3 Interoperability

Repositories used to publish CA certificates and CRLs shall employ standard-based scheme for directory objects and attributes, at least, LDAPv3.

2.3 Time or Frequency of Publication

Certificates issued under LAWtrust PKI Hierarchy are published in the Repository as soon as possible after issuance. CRLs for the Issuing CAs Certificates are issued at least every 6 months and within 24 hours if a CA Certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued.

This CP and any subsequent changes should be made available to the participants as set forth in section 2.2.2 within two weeks of approval by LAWtrust Security Committee.

This CP is provided as public information on the official LAWtrust website. Internal documents are only valid if they are published as a PDF and digitally signed by the LAWtrust Policy Authority.

2.4 Access Controls on Repositories

Certificates and certificate status information in the repository shall be made available to LAWtrust PKI participants and other parties on a 24/7 basis as determined by the applicable agreements and LAWtrust Privacy Policy, and subject to routine maintenance.

LAWtrust will protect repository information not intended for public dissemination or modification using strong authentication, access controls, and an overall Information Security Management System that prevents unauthorized access to information.

The controls employed by LAWtrust shall prevent unauthorized persons from adding, deleting, or modifying repository entries. Access restrictions shall be implemented on directory search to prevent misuse and unauthorized harvesting of information.

This CP and accompanying CPS documents are provided as public documents and not subject to access control restrictions.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Each Certificate must have a unique identifiable Distinguished Name (DN) according to the X.500 standard. Common Names (CN) must be unique within each naming space.

3.1.2 Need for Names to be Meaningful

The Sub-CA certificates and Subscriber certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates are understood and used by Relying Parties.

The LAWtrust Root CA 2048 DN (LDAP Notation) and LAWtrust Root CA2 (4096) in the Issuer field of all certificates and CRLs that are issued will be:

- CN=LAWtrust Root Certification Authority 2048, O=LAWtrust, C=ZA
- CN=LAWtrust Root CA2 (4096),O=LAWtrust, C=ZA

LAWtrust Issuing CAs DN (LDAP Notation) in the Issuer field of all certificates and CRLs that are issued will be:

- CN=LAWtrust AeSign CA 2048, O=LAWtrust, C=ZA
- CN=LAWtrust AeSign CA02, O=LAWtrust, C=ZA
- CN=Lawtrust AATL CA01, O=LAWtrust, C=ZA
- CN=LAWtrust Auth CA02, O=LAWtrust, C=ZA
- CN=LAWtrust Signing CA01, O=LAWtrust, C=ZA
- CN=LAWtrust Auth CA01, O=LAWtrust, C=ZA
- CN=LAWtrust Secure CA01, O=LAWtrust, C=ZA

3.1.3 Anonymity or Pseudonymity of Subscribers

LAWtrust CA(s) may not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

The naming convention used by LAWtrust CA(s) is ISO/IEC 9595 (X.500) Distinguished Name (DN). The LAWtrust PKI may further stipulate how names are to be interpreted by publishing such rules in the applicable CPS.

3.1.5 Uniqueness of Names

All distinguished names shall be unique across LAWtrust CAs.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate applicants are prohibited from using names in their certificate application that infringe upon the Intellectual Property Rights of others. LAWtrust Issuing CAs and their RAs, however, does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application.

LAWtrust Issuing CAs may revoke a Certificate upon receipts of a properly authenticated order from an arbitrator or court of competent jurisdiction requiring the revocation of a Certificate or Certificates containing a Subject name in dispute.

3.2 Initial Identity Validation

LAWtrust Issuing CAs may perform identification of the Applicant for services using any legal means of communication or investigation as necessary to validate the identity of the applicant.

3.2.1 Method to Prove Possession of Private Key

The LAWtrust Root CAs shall accept Certificate Signing Requests (CSR) from the Issuing CAs that have demonstrated possession of the Private Key by using a self-signed PKCS#10 request.

The LAWtrust Issuing CAs generate subscriber keys in a secure manner, or where applicable, accept certificate signing requests in PKCS#10 format.

3.2.2 Authentication of organizational entity

For all certificates issued by LAWtrust CA(s) that include an organization identity, applicants are required to indicate the organization's name and registered or trading address. The legal name and existence thereof must be verified using methods determined in the LAWtrust CPS.

3.2.2.1 Identity-Proofing of End User Subscribers

LAWtrust PKI (or delegated RA) will ensure that the Applicant's identity information is verified. Minimal procedures for authentication of Subscribers are described further in the LAWtrust Issuing CAs CPS and respective verification process applicable to specific certificate types is described in the corresponding LAWtrust Issuing CA CPS document, which is mandated.

3.2.2.2 Identity-Proofing of Organizational Entities

If the subject of the certificate is to include the organization's name, LAWtrust CA(s) or RA(s), as the case may be, shall verify the identity and address of the organization. The organization's address shall also be verified to confirm if it is the same address where the organization conducts its operation. The CA or an RA shall verify these details using documentation provided by the applicant or verifying against any of the following:

- A government agency within the jurisdiction of the organization's legal existence or recognition;
- A third-party database that is periodically updated and considered a reliable data source; or

- An attestation letter written by a lawyer, a judge or other third party that is customarily relied upon for such information

LAWtrust CA or an RA, as the case may be, shall act in accordance with the CPS and all LAWtrust CA collateral documentation. In doing so, it will comply with the corresponding practices, procedures and policies described therein.

For collection and verification of information provided by the applicant, RAs shall follow the processes based on the certificate type requirements defined by the LAWtrust CA.

3.2.3 Non-verified Subscriber Information

Non-verified information shall not be included in certificates issued under LAWtrust Issuing CAs, unless specifically mentioned in the Certificate Types section of the relevant CPS.

3.2.4 Validation of Authority

LAWtrust Security Committee shall, before certificate issuance, ensure that the applicant has specific rights, entitlements, or permissions to obtain a certificate on behalf of the Subordinate CAs and the organization that is the subject of the certificate.

3.2.5 Criteria of Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

For any re-key of the LAWtrust Root CAs or LAWtrust Issuing CAs, a scripted and witnessed processes shall be followed.

Subscribers shall identify themselves to the LAWtrust Issuing CAs using their current Authentication Keys, failing which the same initial validation procedure shall be followed.

For routine re-key of repository (e.g., OCSP) and RA Certificate refer to LAWtrust Operations Policies and Procedures.

3.3.2 Identification and Authentication for Re-key After Revocation

If any one of the LAWtrust Root CA or LAWtrust Issuing CA's are revoked, a key ceremony shall be constituted to regenerate new keys and issue new certificates for the revoked CA after approval by the LAWtrust Security Committee.

If a Subscriber Certificate is revoked, the Subscriber shall go through the same initial identity proofing process as per respective certificate type to obtain a new certificate.

3.4 Identification and Authentication for Revocation Requests

Prior to the revocation of Sub-CA Certificates, LAWtrust Security Committee shall verify that the revocation has been requested by an authorized person and that such a request is approved by LAWtrust Security Committee.

Prior to the revocation of a Subscriber certificate, LAWtrust Issuing CAs shall verify that the revocation has been requested by an entity authorized to request revocation. Acceptable procedures for authenticating the revocation requests are described in the relevant CPS documents.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

LAWtrust Root CAs do not accept external applications for sub-CA certification. LAWtrust Security Committee approves LAWtrust Issuing CAs following internal service requests from authorized personnel.

This section specifies the requirements for initial application for certificate issuance by LAWtrust Issuing CAs through its Registration Authorities. The RA will perform the following steps when an applicant applies for a certificate:

- Establish the applicant's authorization to obtain a certificate;
- Establish and record the identity of the applicant; and
- Transmit to LAWtrust Issuing CAs a confirmation that the Applicant has met the authentication requirements and the information which is to appear in the Certificate.

LAWtrust Issuing CA will perform the following steps when it receives the confirmation and certificate information from the RA:

- Verify that the transmission is from an authorized RA;
- Private key ownership verification to be performed by CA or RA
- Generate the Certificate relating to that Applicant; and
- Transmits the Certificate to the Applicant and/or to the requesting RA.

4.1.1 Submission of Certificate Application

Applications for the establishment of internal Sub-CAs under LAWtrust Root CAs shall be made to LAWtrust Security Committee. LAWtrust Security Committee shall consider the request and advice the requester of the outcome. Final approval shall be signed off by the Policy Authority.

Subscriber certificate applicants, including those applying for an entity certificate, will follow the application process specified in respective certificate type as described in the applicable CPS document.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 Issuing CAs

Prior to the approval and issuance of Sub-CA certificates by LAWtrust Root CAs, LAWtrust Security Committee or the PA, as the case may be, shall obtain the following documentation from the authorized applicant/requestor:

1) Sub-CA establishment request
2) Sub-CA Key Generation Script
3) Other supporting documentation such as a Business Case.

4.1.2.2 Subscribers

Subscribers follow the procedures published by the RAs for certificate application.

4.1.2.3 Registration Authorities/Agents

An entity wishing to become an RA or RA-Agent under the LAWtrust Issuing CA shall agree to the terms of the RA Agreement / RA Agent Agreement as part of the application process. The applicants shall provide their credentials to demonstrate their identity and contact information during the application process.

All applicants shall agree to the terms and conditions of the applicable Agreement, i.e., Registration Authority Agreement or RA-Agent Agreement.

4.2 Certificate Application Processing

4.2.1 Performing Identity-proofing Functions

RAs or RA-Agents shall perform identification and authentication of all required Subscriber information as described in the applicable section of the CPS, for the applicable certificate type.

4.2.2 Approval or Rejection of Certificate Applications

LAWtrust Security Committee may approve requests for Sub-CA establishment after considering the application. The committee may also reject the establishment of Sub-CAs when requisite information is not provided in the application or for any other reason that the committee may deem fit.

The RA or RA-Agent will approve an application for a subscriber certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information as described in the applicable CPS, for each respective certificate type.

The RA or RA-Agent will reject a certificate application if:

- Identification and authentication of all required Subscriber information as described in the Subscriber Agreement cannot be completed;
- The Subscriber fails to furnish supporting documentation upon request;
- The Subscriber fails to respond to notices within a specified time; or
- The RA believes that issuing a certificate to the Subscriber may bring LAWtrust Issuing CA into disrepute;
- The applicant fails to prove private key ownership.

Policies specific to each certificate type have been detailed in the Certificate Types section in the applicable CPS. It is mandatory to comply with all policies specific to the respective certificate type.

4.2.3 Time to Process Certificate Applications

LAWtrust Security Committee shall process the Root, Issuing and RA certificates applications as soon as is reasonably possible after receipt of such applications.

Certification applications are processed within a commercially reasonable time in accordance with the CPS or any agreement signed with the PKI participants. LAWtrust Issuing CAs shall not be held liable for any processing delays initiated by the applicant or for events outside the CAs' control.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

LAWtrust PKI under the LAWtrust Security Committee shall verify the source of the Sub CA certificate request before issuance. Once the authenticity of the application is confirmed, the LAWtrust Root CA will create and sign the Sub-CA certificate provided all certificate requirements (including correct population of the certificate fields and extensions) as described in the Key Ceremony Script have been met.

When RAs/RA-agents receive a request for Certificate, it is not issued before the applicant accepts the terms of a Subscriber Agreement, successfully completes the application form and the request has been successfully validated using mechanisms such as validating the digital signature of the RA.

Following successful completion of the registration process, the LAWtrust Issuing CAs will create and sign the certificate if all certificate requirements have been met and make the certificate available to the subscriber.

4.3.2 Notification of Certificate Issuance

LAWtrust Root CAs shall notify the applicant of the Sub-CA immediately, as the issuance forms part of a scripted and witnessed Key Ceremony process.

LAWtrust Issuing CAs shall notify Subscribers, either directly or through the RA/RA-Agent, that they have created the Subscribers Certificate and provide Subscribers with access to the Certificates by notifying them that their Certificates are available as defined in the CPS.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

On receipt of the signed certificate from the LAWtrust Root CA, the Sub-CA may be established, and this action constitutes acceptance of the certificate by the Sub-CA.

The use of the Sub-CA Certificate or the reliance upon the Certificate signifies acceptance by that person of the terms and conditions of the CP and applicable agreements by which they irrevocably agree to be bound.

Certificate acceptance is governed by the agreements set out between the RA/RA-Agent and Applicants, any requirements imposed by LAWtrust CP and CPS together with the relevant agreements under which the certificate is being issued.

4.4.2 Publication of the Certificate by the CA

Certificates will be published, once accepted, in the appropriate repository as described in section 2.1.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Private Key and Certificate Usage

Sub-CAs may only use the Private Key and associated public key contained in the certificate once accepted. The Sub-CAs shall only use their Private Keys for the purposes as contained in the Sub-CA certificate extensions such as key usage, extended key usage, certificate policies etc.

Subscribers shall use their Certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of the Subscriber Agreement, this CP, and applicable laws. Subscribers shall protect their Private Keys from access by any other party

and shall notify the CA or RA, upon the compromise of the private key or any reasonable suspicion of compromise.

Subscribers shall discontinue use of private key(s) following expiration or revocation of the associated certificate

4.5.2 Relying Party Public Key and Certificate Usage

The Relying Party Agreement becomes effective when the Relying Party relies on information provided by LAWtrust Root CAs, LAWtrust Issuing CAs or a subscriber regarding a specific transaction that the Relying Party uses to accept or reject their participation in the transaction.

The Relying Party's use of the Repository, or any CRL or certificate status services is governed by the Relying Party Agreement and LAWtrust CP. The Relying Party is solely responsible for deciding whether or not to rely on the information in a certificate provided by LAWtrust Root CAs or LAWtrust Issuing CAs. The Relying Party bears the legal consequences of any failure to comply with the obligations set in the Relying Party agreement.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. Certificate renewal is supported for LAWtrust Root CAs issued certificates to Sub-CAs and LAWtrust Issuing CAs issued certificates to Subscribers.

4.6.1 Circumstances for Certificate Renewal

LAWtrust Root CAs and LAWtrust Issuing CAs may renew Sub-CA and Subscriber certificates provided the following conditions are met:

- The original Sub-CA or Subscriber certificate to be renewed has not been revoked;
- The details in the original Sub-CA or Subscriber certificate remains accurate and that no new or additional validation is required.

Should the above not be met, a new Sub-CA or Subscriber certificate must be issued following the normal Key Generation process for a new Sub-CA or Subscriber certificate.

4.6.2 Who may request Certificate Renewal

The request for renewal may only be made by a person in a role authorized to do so, such as LAWtrust Policy Authority, RA, RA-agent or the subscriber themselves.

4.6.3 Processing Certificate Renewal Requests

The renewal request may only be processed after receiving such a renewal request from the original authorized representative or proxy. LAWtrust Security Committee shall process all Sub-CA or Subscriber Certificate Renewal Requests after satisfying itself of the authenticity and validity of the request.

4.6.4 Notification of Renewed Certificate Issuance

Sub-CA or Subscriber certificate renewals shall follow the same notification method as a new Sub-CA or Subscriber certificate issuance.

4.6.5 Conduct constituting acceptance of a renewal certificate

Sub-CA or Subscriber renewal certificate acceptance shall follow the same conditions for a new Sub-CA or Subscriber acceptance.

4.6.6 Publication of a Renewal Certificate

The Sub-CA or Subscriber renewed certificate shall be published at the same location as the original certificate.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Generally, LAWtrust CAs do not notify other entities of a renewed Sub-CA certificate apart from requesting party.

4.7 Certificate Re-Key

Re-keying a certificate (key update) refers to the issuance of new certificate with a different key pair and serial number while retaining other subject information from old certificate.

The new Certificate may be assigned a different validity period and/or signed using a different issuing CA private key.

4.7.1 Circumstances for Certificate Re-key

Manual certificate re-key for the Issuing CAs (level-2 CAs) shall be performed within three months of certificate expiry. The process shall be a witnessed key ceremony process similar to the initial key generation and certificate issuance.

LAWtrust Issuing CAs may re-key certificates provided that the following conditions are met:

- The certificate to be re-keyed must not have been revoked;

- All details of the certificate remain accurate and no new validation of identity is required.

4.7.2 Who can Request a Certificate Re-key

In accordance with the conditions specified in previous section, Certificate re-key may be requested by an authorized person within LAWtrust. LAWtrust Security Committee shall approve all Sub-CA certificate re-key requests.

Certificate re-key may be requested by:

- An RA for its own RA certificate
- A subscriber for his own individual certificate
- An authorized representative for an Organizational certificate.

4.7.3 Processing Certificate Re-keying Requests

Processing of Sub-CA certificate re-keying request shall be initiated only after successful verification of the re-key request from a LAWtrust authorized representative; in each case the LAWtrust Security Committee shall approve all re-key requests.

Only after verifying re-key request from subscriber or authorized representative; processing of certificate re-keying request shall be initiated.

4.7.4 Notification of a Re-keyed Certificate Issuance

Notification of issuance of a re-keyed certificate by LAWtrust Root CAs to Relying Parties shall follow the same procedures as notification for newly issued Sub-CA certificates.

Notification of issuance of a re-keyed certificate by LAWtrust Issuing CAs to Subscribers shall follow the same procedures as notification for newly issued certificates.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Conduct constituting acceptance of a re-keyed certificate is same as listed in section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

After successful completion of the re-key process, the certificate shall be published in appropriate repositories, in the same manner as for a newly issued certificate.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Generally, LAWtrust CAs do not notify other entities of a re-keyed certificate apart from the requesting LAWtrust representative.

4.8 Certificate Modification

LAWtrust Root CAs and LAWtrust Issuing CAs do not support any form of Sub-CA or Subscriber certificate modification. The issued Sub-CA/Subscriber certificate must first be revoked, and a new process followed to re-issue the certificate using the same process as for initial issuance.

4.9 Certificate Revocation and Suspension

A Certificate shall be revoked/suspended when the binding between the Subject and the Subject's Public Key defined within a Certificate is no longer considered valid.

The LAWtrust Root and Issuing CAs will notify other participants of certificate revocation or suspension through access to the CRL (or OCSP) in the CA repository.

The Issuing CA and/or RA will notify subscribers of certificate revocation or suspension using any of the below methods:

- Access to the CRL in the CA repository;
- Via the OCSP method where applicable;
- Email notification to subscriber (Such notification is deemed complete, once the email is sent by LAWtrust Issuing CA to the subscriber's registered email address); or
- Internal communication mechanisms will be used to notify subscribers.

4.9.1 Circumstance for Revocation of a Certificate

LAWtrust Root CAs shall revoke subordinate Issuing-CA (Sub-CA) Certificates for the following non-exhaustive reasons:

- LAWtrust Root CA suspects or determines that the Sub-CA Private Key is compromised.
- LAWtrust Root CA suspects or determines that revocation of a Sub-CA Certificate is in the best interest of the integrity of LAWtrust PKI Hierarchy;
- LAWtrust Root CA determines that a Certificate was not issued correctly in accordance with this CP;

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed in a CRL.

LAWtrust Issuing CAs shall revoke Certificates of Subscribers for the following non-exhaustive reasons:

- The Subscriber has failed to meet its obligations under this CP or any other applicable Agreements, regulations, or laws;

- The LAWtrust Issuing CA suspects or determines that revocation of a Certificate is in the best interest of the integrity of LAWtrust;
- The LAWtrust Issuing CA determines that a Certificate was not issued correctly in accordance with this CP;
- There has been an improper or faulty issuance of a certificate due to:
    - A material prerequisite to the issuance of the Certificate not being satisfied;
    - A material fact in the Certificate is known, or reasonably believed, to be false.
- The subscriber of the Certificate or his authorized agent asks for their Certificate to be revoked due to:
    - The Subscriber's private key is suspected to be compromised;
    - The cryptographic storage device of the Subscriber is lost or stolen;
    - If the subscriber no longer wishes to use the certificate.
- LAWtrust Issuing CA to revoke the certificate of the subscriber, if the subscriber is no longer part of the organization; or
- The Registration Authority's Agreement has been terminated.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a CRL and/or specified as revoked by an OCSP Responder.

4.9.2 Who Can Request Revocation of a Certificate

The following entities can request revocation of a certificate:

- LAWtrust can request the revocation of any certificates issued by any CA participating in the LAWtrust PKI;
- The LAWtrust Security Committee can request the revocation of any of the Sub-CA certificates issued under LAWtrust PKI Hierarchy;
- LAWtrust PA can request the revocation of any certificates issued under its authority;
- An RA for their own certificate, if any suspected misuse has been attributed to their given Certificates;
- Subscribers, if any suspected misuse has been attributed to their given Certificates, can request a revocation.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The LAWtrust Root and Issuing CAs shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements. LAWtrust Security Committee has the final approval for the revocation of Sub-CA certificates.

4.9.4 Revocation Request Grace Period

Revocation request grace period is not permitted once a revocation request has been verified.

4.9.5 Time within which CA must Process the Revocation Request

LAWtrust Root CA shall process authorized revocation requests within 24 hours whereas LAWtrust Issuing CAs shall process authorized revocation requests within a commercially reasonable time.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties should comply with the signature validation requirements defined in the Relying Party Agreement.

4.9.7 CRL Issuance Frequency

LAWtrust Root CAs shall issue CRLs at least every 6 months and within 24 hours after revocation of an Issuing CA.

LAWtrust Issuing CAs shall issue CRLs within 24 hours after revocation of a Subscriber certificate.

4.9.8 Maximum Latency of CRLs

CRLs shall be published in the Repositories within 24 hours of Certificate revocation.

4.9.9 Online Revocation Checking Availability

There shall be no online revocation checking for the LAWtrust Root CAs.

LAWtrust Issuing CAs may provide access to an OCSP Responder covering the certificates they issue. The OCSP responses shall conform to RFC 6960 and the OCSP responder's certificate must be signed by the LAWtrust Issuing CAs.

The OCSP service shall be available 24 hours a day with reasonable time allocated to maintenance.

4.9.10 Online Revocation Checking Requirements

LAWtrust Issuing CAs shall provide Online revocation and status checking to its relying parties. LAWtrust Issuing CAs shall update information provided via an OCSP at least every four days.

The OCSP responses from this service will not exceed an expiration time of ten days. OCSP Responders that receive a request for status of a Certificate that has not been issued, shall not respond with a “good” status for such Certificates.

LAWtrust Issuing CAs shall require OCSP requests to contain the following data:

- Protocol Version
- Service request
- Target certificate identifier

4.9.11 Other Forms of Revocation Advertisements Available

LAWtrust Root CAs will not provide other forms of revocation advertisements other than CRLs.

LAWtrust Issuing CAs will not provide other forms of revocation advertisements, other than OCSP and CRL.

4.9.12 Special Requirements Related To Key Compromise

If LAWtrust PKI discovers, or has a reason to believe, that there has been a compromise of the private key of the LAWtrust Root CA or any Issuing CA, LAWtrust PKI will immediately declare a disaster and invoke the Business Continuity Plan. LAWtrust PKI will

1) Determine the scope of certificates that must be revoked,
2) Revoke the affected certificates as per LAWtrust PKI procedures,
3) Publish a new CRL as stipulated in section 4.9.7,
4) Generate new CA key pair as per LAWtrust operations policies and procedures.

4.9.13 Circumstances for Certificate Suspension

LAWtrust Issuing CAs have the option to suspend Certificates under the circumstances described in section 4.9.1.

4.9.14 Who Can Request Suspension

- LAWtrust can request the suspension of any certificates issued by any CA participating in the LAWtrust PKI;
- The LAWtrust PA, LAWtrust Operations Authority or LAWtrust Security Committee can request the suspension of any certificate issued under its authority;

- An RA can request the suspension of one of their Subscribers Certificate;
- Subscribers, if any suspected misuse has been attributed to their given Certificates, can request a suspension; and
- A legal, judicial or regulatory agency can request a suspension.

If any request for suspension cannot be resolved for whatever reason, the request is subject to the Dispute Resolution process described in the LAWtrust Dispute Resolution Policy.

4.9.15 Procedure for Suspension Request

A request to suspend a certificate shall identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally, or manually signed).

LAWtrust Issuing CA or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements.

For Suspension of RA Certificates, LAWtrust Security Committee shall approve any such suspension.

Once suspended, the serial number of the Certificate and the date and time shall be added to the appropriate CRL and a reason code of "**on hold**" will be included in the CRL.

4.9.16 Limits on Suspension Period

The maximum period for which a Certificate can be suspended will be defined by the LAWtrust CA Policy Authority but shall not exceed the validity of the certificate.

4.9.17 Circumstances for Terminating Suspended Certificates

A suspended Certificate is reactivated when the entity which requested the suspension of a Certificate is satisfied that the circumstances leading to the suspension are no longer valid. Once reactivated, the certificate will be valid for the remainder of its initial lifetime.

A suspended Certificate is revoked when the entity which requested the suspension of a Certificate is satisfied that the circumstances leading to the suspension are indeed valid.

When the period for suspension has reached its maximum duration without resolution, the certificate will be revoked.

4.9.18 Procedure for Terminating the Suspension of a Certificate

A request to unsuspend a certificate shall identify the certificate to be unsuspended, explain the reason for unsuspension, and allow the request to be authenticated (e.g., digitally or manually signed).

LAWtrust Issuing CA or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements.

4.10 Certificate Status Services

The status of LAWtrust Issuing CAs public certificates is available from CRLs in the repositories and via OCSP responder services (where available).

LAWtrust Issuing CAs shall keep the revocation on the CRL or OCSP until after the expiry date of the revoked certificate.

4.11 End of Subscription

Subscribers may end their subscription to certificate services by having their subscriber certificate revoked or letting it expire naturally.

4.12 Key Escrow and Recovery

LAWtrust Root CAs and Issuing CAs does not provide a Key Escrow service.

5. FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Security Controls

LAWtrust operates the LAWtrust PKI (Root and Issuing CAs), Repositories and OCSP responder at the LAWtrust data center, with appropriate physical and procedural access controls for all hardware and software sub-systems used in the issuance and revocation of certificates. LAWtrust limits access to functions critical to registration and certificates to personnel in Trusted Roles.

LAWtrust shall have physical and environmental security policies for systems used for certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery. Controls should be implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities

5.1.1 Site Location and Construction

The location and construction of the facility housing LAWtrust Root CAs, LAWtrust Issuing CAs and LAWtrust Data Center equipment is consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other

physical security protection mechanisms such as guards and intrusion sensors, provides robust protection against unauthorized access to LAWtrust CAs' equipment and records.

5.1.2 Physical Access

LAWtrust Root and Issuing CAs' systems are protected by at least four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Progressively restrictive physical access privileges control access to each tier. Sensitive LAWtrust CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Physical access is automatically logged, and video recorded. Additional tiers enforce individual access control through the use of biometric authentication. Unescorted personnel, including un-trusted employees or visitors, should not be allowed into such secured areas. The facility hosting CA equipment is monitored on a 24x7 basis. Normal and emergency lighting are provided to the CA facilities.

LAWtrust shall ensure that the facilities used for the Issuing CA Certificate life cycle management are operated in an environment that physically protects the services from compromise through unauthorized access to systems or data. An authorized employee should always accompany any unauthorized person entering a physically secured area. Physical protections should be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting LAWtrust PKI operations. No parts of LAWtrust PKI premises shall be shared with other organizations within this perimeter.

5.1.3 Power and Air Conditioning

LAWtrust shall ensure that the power and air conditioning facilities are sufficient to support the PKI Operations environment.

The LAWtrust PKI equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Any of the LAWtrust CA on-line servers (e.g., CAs hosting directories) shall be provided with Uninterrupted Power sufficient to support a smooth shutdown of the PKI operations.

5.1.4 Water Exposure

LAWtrust shall ensure that LAWtrust PKI CA systems are protected from exposure to water sources.

5.1.5 Fire Prevention and Protection

LAWtrust PKI CAs equipment shall be housed in a facility with appropriate fire suppression and protection systems.

5.1.6 Media Storage

LAWtrust shall ensure that LAWtrust PKI CAs media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive or backup information is duplicated and stored in a location separate from the operational CAs.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations are destroyed using appropriate disposal processes as defined in LAWtrust Sensitive data disposal policy.

5.1.8 Off-Site Backup

Full system backups of CAs, sufficient to recover from system failure, are made on a periodic schedule as described in LAWtrust Operations Policies and Procedures.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of LAWtrust PKI. The following are the trusted roles for LAWtrust PKI:

- CA Administrator – general CA administration and approval of the generation, revocation and suspension of certificates
- CA Security Officer – overall responsibility for administering the implementation of the CA's security practices, cryptographic key lifecycle management functions
- CA Policy Authority – responsible for the overall development, maintenance and ensures approval of CA policies
- CA Operations Authority – responsible for the implementation of the CA policies and development of operational procedures and guidelines
- CA Auditor – internal auditor is responsible for ensuring the CA is operating in line with approved policies and procedures. The auditor is also responsible for checking that procedures are being followed correctly during Key Ceremonies
- CA Key Manager – responsible for CA Key Lifecycle management functions
- CA Key Shareholders – holders of the CA key components
- CA Developers – responsible for the development of CA systems

- CA Operators – Responsible for the day-to-day operation and maintenance tasks on the system.

5.2.2 Number of Persons Required per Task

LAWtrust shall ensure separation of duties for critical CA functions to prevent one person from maliciously using the PKI systems without detection. Each user's system access is limited to those actions for which they are required to perform in fulfilling their responsibilities. Separate individual shall fill each of the roles specified in LAWtrust Trusted Roles document. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over the system operation.

A single person may be sufficient to perform tasks associated with a role, except for the activation of the CA certificate signing Private Key. Activation of the CA certificate signing Private Key shall require M/N protection (i.e. actions by any two (2) out of three people (3)).

5.2.3 Identification and Authentication for Each Role

An individual shall identify and authenticate themselves before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Separation of Roles

Individual CA personnel are specifically designated to the roles defined in section 5.2.1 of this CP and LAWtrust Trusted Roles document. LAWtrust PKI will ensure that the segregation of duties is maintained when assigning trusted roles to individuals.

5.3 Personnel Controls

5.3.1 Qualifications, Experience And Clearance Requirements

All persons filling trusted roles shall be selected based on skills, experience, loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA are set forth in the LAWtrust Trusted Roles document and LAWtrust Organization Structure document.

5.3.2 Background Check and Clearance Procedures

LAWtrust conducts background investigations for all LAWtrust PKI personnel including trusted roles and management positions.

The LAWtrust on boarding process includes the following checks

:

- Employment Reference check
- Education certificates check
- Criminal Check.

Security clearance shall be repeated every 3 years for personnel holding trusted roles. All persons filling the Trusted Roles shall only be granted access to the LAWtrust PKI systems once the background clearance procedures detailed above have been completed and confirmed.

5.3.3 Training Requirements

LAWtrust shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as basic Public Key Infrastructure knowledge, security requirements, operational responsibilities and associated procedures.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for PKI roles are made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

LAWtrust Personnel should be retrained when a new version of software or underlying hardware platform is being planned for operations or every two years whichever is realised first.

5.3.5 Job Rotation Frequency and Sequence

LAWtrust PKI shall ensure that any change in the staff complement will not affect the operational effectiveness of the PKI services and security thereof.

5.3.6 Sanctions for Unauthorized Actions

LAWtrust PKI shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions (i.e., not permitted by the CP, CPS and/or other procedures) involving LAWtrust PKI or its repository.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to LAWtrust PKI Operations shall be subjected to the same processes, sanctions, assessment, security and operational

procedure as permanent personnel, under adequate supervision and perform only assigned tasks.

5.3.8 Documentation Supplied to Personnel

LAWtrust will make available to its personnel its CP, CPS, and any relevant documents required to perform their duties.

5.4 Audit Logging Procedures

Audit log files are generated for all events relating to the security of LAWtrust Root and Issuing CAs, and other associated components. The security audit logs for each auditable event defined in this section are maintained in accordance with onsite retention period and for archive.

5.4.1 Types of Events Recorded

LAWtrust PA shall ensure recording in audit log files all events relating to the security of the CA system hosted in LAWtrust data centre. All security audit capabilities of the CA operating system and CA applications shall be enabled. Such events include, but are not limited to:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. Issuing CA Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, suspension and revocation;
    b. All verification activities stipulated in these Requirements and the Issuing CA's Certification Practice Statement;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of Certificates; and
    f. Generation of Certificate Revocation Lists.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed, such as:
        - the value of maximum authentication attempts is changed;
        - an administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts

c. Security profile changes;
d. System crashes, hardware failures, and other anomalies;
e. Firewall and router activities;
f. Entries to and exits from the LAWtrust PKI facility;
g. Equipment failure or electrical power outages; and
h. Changes to CA configuration and system clock time

Log entries MUST include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry; and
- Description of the entry.

All logs, whether electronic or manual, must contain the date and time of the event and the identity of the Entity which caused the event. The CA shall also collect, either electronically or manually, security information not generated by the CA system such as:

- Physical access logs;
- System configuration changes and maintenance;
- CA personnel changes;
- documentation relating to certificate requests and the verification;
- documentation relating to certificate revocation;
- Discrepancy and No compromise reports;
- Information concerning the destruction of sensitive information;
- Current and past versions of all Certificate Policies;
- Current and past versions of Certification Practice Statements;
- Vulnerability Assessment Reports;
- Threat and Risk Assessment Reports;
- Compliance Inspection Reports; and
- Current and past versions of Agreements.

5.4.2 Frequency of Processing Data

Audit logs are required to be processed periodically in accordance with LAWtrust Audit and Compliance Policy.

5.4.3 Retention Period for Audit Log

LAWtrust Root and Issuing CAs shall retain all system generated (electronic and manual) audit records onsite for a period not less than twelve months from the date of creation.

5.4.4 Protection of Audit Log

LAWtrust Root and Issuing CAs shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

5.4.5 Audit Log Backup Procedures

LAWtrust Root and Issuing CAs shall back up all audit logs and audit summaries in a secure location and protected to the same degree as the originals.

5.4.6 Audit Collection System (Internal or External)

The audit collection system may be an internal system. The audit collection system must maintain integrity and availability of the data collected as detailed in the LAWtrust Audit and Compliance Policy.

5.4.7 Notification to Event-Causing Subject

Event-causing subject are not notified.

5.4.8 Vulnerability Assessments

Routine vulnerability assessments of security controls shall be performed by LAWtrust for its Root CA, Issuing CAs and other PKI supporting systems hosted in the LAWtrust data centre.

The LAWtrust security program must include an annual Risk Assessment which includes identification of foreseeable internal and external threats, assess the likelihood and potential damage of these threats and assess the sufficiency of the policies, procedures, information systems and technology. The program must also ensure vulnerability assessments are performed, reviewed and revised following an examination of audit events.

Based on the Risk Assessment exercise, LAWtrust shall develop, implement, and maintain a security plan to control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

5.5 Records Archival

5.5.1 Types of Events Archived

LAWtrust PKI archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA. LAWtrust PKI shall make these archived records available to its Qualified Auditor upon request. The details of the events to be archived shall be described in the CPS.

5.5.2 Retention Period for Archive

The minimum retention periods for archive data are established in accordance with applicable regulatory guidance, laws, Agreements, and as specified by LAWtrust PA. LAWtrust PKI CA's minimum retention period for archive data is established at 7 years.

LAWtrust PKI CAs shall retain all documentation relating to LAWtrust PKI CAs certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least 7 years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

Only authorized individuals shall be permitted to review the archive. The contents of the archive shall not be released except as determined by LAWtrust, LAWtrust PA, or as required by law. Records and material information relevant to use of, and reliance on, a certificate shall be archived. Archive media shall be stored in a secure storage facility separate from the component itself. Any secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism. Data to be migrated periodically to fresh media; and protection against obsolescence of hardware, operating systems, and other software, by, for example, retaining as part of the archive the hardware, operating systems, and/or other software to permit access to and use of archived records over time.

5.5.4 Archive Backup Procedures

Only one copy of the archive is maintained. In other words, archive itself is not backed up.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. System logs shall be time stamped and systems use a dedicated time server to maintain synchronized time.

5.5.6 Archive Collection System

No Stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No Stipulation.

5.6 Key Changeover

The CA system utilized by LAWtrust PKI may periodically perform key rollover, allowing CA keys to be changed periodically as required to minimize risk to the integrity of LAWtrust PKI. Once changed, the new key is used for certificate signing purposes. The unexpired older keys are used to sign CRL's until all certificates signed by the unexpired older private key have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If LAWtrust Root or Issuing CAs detects a potential hacking attempt or other form of compromise to the CA, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in LAWtrust Operations Policies and Procedures shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if LAWtrust Root or Issuing CAs needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

LAWtrust PKI CAs shall maintain backup copies of hardware, system, databases, and private keys in order to rebuild LAWtrust PKI capability in case of software and/or data corruption.

5.7.3 CA Private Key Compromise Recovery Procedures

LAWtrust PKI shall develop and maintain Recovery Policies and Procedures. Same shall be followed in the case of LAWtrust Root or Issuing CAs Private Key compromise.

5.7.4 Business Continuity Capabilities after a Disaster

LAWtrust PKI shall develop robust Business Continuity Management System for critical PKI services in order to provide the minimum acceptable level of assurance to its subscribers for service availability.

All LAWtrust critical infrastructure equipment at the primary site shall have built-in hardware fault-tolerance and configured to be highly available with auto-failover switching. LAWtrust shall maintain copies of backup media and infrastructure system software, which include but

are not limited to PKI services related critical data; database records for all certificates issued and audit related data, at its offsite business continuity and disaster recovery storage facilities.

Business Continuity Management components at LAWtrust PKI shall be regularly tested, verified, and updated to be operational to address crisis situation in the event of a disruption.

LAWtrust PKI shall develop Disaster recovery plans to mitigate the effects of any kind of natural, man-made or equipment failure related disaster.

LAWtrust PKI shall implement an alternate recovery site as per industry standards to provide full recovery of critical PKI services within one week following a disaster at the primary site.

5.8 CA OR RA Termination

5.8.1 CA Termination

When it is necessary to terminate any of LAWtrust PKI CA operations, the impact of the termination must be minimized as much as possible in light of the prevailing circumstances and is subject to the applicable LAWtrust PKI Agreements. Procedures to be followed for the termination of LAWtrust PKI CA operations shall be developed, and must at a minimum include the following:

- Ensure minimal disruption caused by the termination of the CA
- Ensure notification of Sub-CAs, Relying Parties and other relevant Stakeholders
- Ensure certificate status information services are provided and maintained for the duration of the termination
- Ensure process for revoking certificates are maintained

LAWtrust shall nominate a custodian of the LAWtrust PKI CAs archival records in case of LAWtrust PKI CA termination.

Should a successor CA be appointed to take over the functions of the terminated LAWtrust PKI CA, such a successor shall, to the extent as it is practical and reasonable, assume the same rights, obligations and duties as the terminated LAWtrust PKI CA.

5.8.2 RA Termination

In the event of LAWtrust Issuing CA terminating an RA, the termination shall be done in such a way to minimize the impact of the termination to the subscribers. Procedures for the termination of the CA shall be developed and shall at minimum address the following:

- Ensure minimal disruption caused by the termination of the RA
- Ensure notification of Subscribers, Relying Parties and other relevant Stakeholders
- Ensure process for revoking certificates are maintained

LAWtrust Issuing CA shall ensure certificate records maintained by the terminated RA are kept secure and available.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pair generation for LAWtrust PKI CAs will be witnessed and attested to by a party separate from LAWtrust PKI CA operator or the CA administrator as mentioned in the Key Generation Script for each CA.

Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. LAWtrust PKI CAs shall use Hardware Security Modules (HSMs) for CA key generation and storage. HSM's should be minimum FIPS 140-2 Level 3 validated.

LAWtrust Root CAs and Issuing CAs key pair generation is performed by multiple trusted personnel using trustworthy systems and processes that provide security and required cryptographic strength for the generated keys.

LAWtrust Root and Issuing CAs key pair is generated in pre-planned Key Generation Ceremony in accordance with the requirements of LAWtrust. The activities performed during the Key Generation Ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by LAWtrust PKI management.

For Subscriber and RA Private keys generated in cryptographic hardware, the key pairs will be generated or protected, as the case may be, in cryptographic modules at least compliant to FIPS 140-2 Level 2 or higher. Keypairs generated in Software shall be generated using trustworthy computer systems.

6.1.2 Private Key Delivery to Subscribers

LAWtrust Root CAs do not generate nor issue subscriber private keys or certificates.

LAWtrust Issuing CAs shall deliver subscriber private keys in a secure format, such as in cryptographic tokens or smartcards when those keys are generated in cryptographic hardware. Subscriber and RA keys generated in Software shall be delivered securely using secure standards such as PKCS#12 file format.

6.1.3 Public Key Delivery to Certificate Issuer

LAWtrust PKI CA shall accept Issuing CA Public Keys that are cryptographically protected, such as those using PKCS#10 mechanisms from an authorized LAWtrust representative. Such Public Key delivery shall be made as part of the Key Ceremony and as documented in the Key Ceremony Script.

6.1.4 CA Public Key Delivery to Relying Parties

LAWtrust Root CAs' Public Key shall be delivered to the Issuing CAs as part of the trust anchor or chain during the Key Ceremony, using the same scheme of the Issuing CA public key delivery to the Relying Parties.

LAWtrust Issuing CAs' Public Key shall be delivered to the Relying Parties by making it available in the repository, https://www.lawtrust.co.za/repository.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. Key sizes are described as below for CAs under LAWtrust PKI. All FIPS-approved signature algorithms shall be considered acceptable. If LAWtrust Security Committee determines that the security of a particular algorithm may be compromised, it shall direct LAWtrust PKI to revoke the affected certificates.

All certificates issued to Issuing CAs shall use at least 2048-bit RSA, in accordance with FIPS 186-5 or equivalent.

The key lengths under the LAWtrust PKI Hierarchy are as follows:

- LAWtrust Root CA 2048: 2048 bits
- LAWtrust Root CA2 4096: 4096 bits
- LAWtrust AeSign Certification Authority 2048: 2048 bits
- LAWtrust AeSign CA02: 2048 bits
- LAWtrust AATL CA01: 2048 bits
- LAWtrust AUTH CA02: 2048 bits
- LAWtrust Signing CA01: 4096 bits
- LAWtrust AUTH CA01: 4096 bits
- LAWtrust Secure CA01: 4096 bits

All certificates issued to subscribers shall use at least 2048-bit RSA, with Secure Hash Algorithm version 2 (SHA-256) in accordance with FIPS 186-5 or equivalent.

The key lengths of certificates issued by LAWtrust Issuing CAs are as follows:

- Subscriber Key Pairs: 2048 bits RSA
- RA Key Pairs: 2048 bits RSA
- OCSP Key Pair: 2048 bits RSA

6.1.6 Public Key Parameters Generation and Quality Checking

The LAWtrust Root CAs shall generate key pairs that comply with FIPS 186-5 and shall use reasonable techniques to validate the suitability of the Sub-CA key pairs.

The LAWtrust Issuing CAs shall generate key pairs that comply with FIPS 186 and shall use reasonable techniques to validate the suitability of the Subscriber key pairs.

6.1.7 Key Usage Purposes

Public keys that are bound into certificates shall be certified for use in authenticating or signing, as specified by LAWtrust. The use of a specific key is determined by the key usage extension in the X.509 certificate. LAWtrust Root CA key is used for certificate and CRL signing. LAWtrust Issuing CA key is used for authentication, confidentiality and digital signature.

6.2 Private Key Protection and Crypto-Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Cryptographic modules, smartcards or tokens employed for subscriber, OCSP Responder, RA private key protection issued by LAWtrust PKI CA shall comply with FIPS-PUB 140-2 “Security Requirements for Cryptographic Modules”, Level 3 and above.

6.2.2 CA Private Key Multi-Person Control

Using of any CA Private signing keys shall require action by multiple persons. LAWtrust Root CA keys can only be accessed on the physical and logical level by adhering to the multi-person control scheme (M out of N) as described in the CPS.

RAs, OCSP Responder and subscribers’ private keys are not under multi-person control.

6.2.3 Private Key Escrow

LAWtrust PKI CAs do not escrow Sub-CA Private keys, RA, Subscriber or OCSP Responder Private keys.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Signing Private Key

LAWtrust Root and Issuing CAs shall backup Private Keys under the same multi-person control scheme as the original Private Keys. The security of the location where the backup keys are kept shall be at the same or higher level as the primary operations site.

6.2.5 Private Key Archival

LAWtrust PKI CAs do not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

LAWtrust PKI CA shall generate, activate and store private keys in FIPS 140-2 Level 3 or above rated Hardware Cryptographic Modules. When the Private Keys are outside the HSM, they shall be kept in encrypted form.

LAWtrust PKI CA keys can be cloned for secure backup from the master hardware cryptographic module to other hardware cryptographic module(s) using secure mechanisms so that they can be recovered if a major catastrophe destroys the productive set of keys.

The LAWtrust Issuing CAs do not permit RAs, OCSP Responder or subscriber key transfer into and out of cryptographic modules or devices. RAs, OCSP Responder and Subscriber keys that are generated in secure cryptographic devices and shall not be transferred out of those devices.

6.2.7 Private Key Storage on Cryptographic Module

LAWtrust PKI CA's Private Key shall be stored on FIPS 140-2 Level 3 validated cryptographic module in encrypted form.

The RAs, OCSP Responder and subscriber keys shall be stored in FIPS 140-2 level 2 devices High Level of Assurance compliant certificates.

6.2.8 Method of Activating Private Keys

LAWtrust PKI CA's private key shall be activated by the main stakeholders and authorized personnel, as defined in LAWtrust Operations Policies and Procedures, supplying their activation data. Such activation data shall be held on secure media and shall require the successful completion of a multi-person authentication process.

Subscriber Private keys shall be activated by providing a passphrase set on initial certificate generation by the subscriber.

6.2.9 Methods of Deactivating Private Keys

LAWtrust PKI CA's private key shall be deactivated by the main stakeholders and authorized personnel, as defined in LAWtrust PKI Operations Policies and Procedures by removing their secure media and storing it in a secure container or environment when not in use.

Subscriber private keys that have been activated shall not be left unattended. Subscribers are obliged to deactivate the private key by "logging out" of the cryptographic device or automatically after a period of inactivity as configured.

6.2.10 Methods of Destroying Private Keys

LAWtrust PKI CA keys shall be destroyed as per CA Termination scripts.

6.2.11 Cryptographic Module Rating

As described in section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archive

The LAWtrust PKI CA and subscriber Public Key is archived as part of the certificate archive process.

6.3.2 Certificate Operational Periods and Key Usage Periods

The table below details key usage, length and certificate lifetime for the corresponding keys:

Key/Certificate	Key Length in Bits	Maximum Validity Period
LAWtrust Root CA 2048 signing key and certificate	2048	20 years
LAWtrust Root CA2 4096 Signing Key and Certificate	4096	30 years
LAWtrust AeSign Certification Authority 2048 Signing Key and Certificate	2048	10 years
LAWtrust AeSign CA02 Signing Key and Certificate	2048	10 years
LAWtrust AATL CA01 Signing Key and Certificate	2048	10 years
LAWtrust Auth CA02 Signing Key and Certificate	2048	9 years
LAWtrust Signing CA01 Signing Key and Certificate	4096	10 years
LAWtrust Auth CA01 Signing Key and Certificate	4096	10 years
LAWtrust Secure CA01 Signing Key and Certificate	4096	10 years
Subscriber Keys	2048	3 years
RA Keys	2048	2 years
OCSP Signing Key	2048	2 years

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock private keys, RA, OCSP responder or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected.

6.4.2 Activation Data Protection

LAWtrust CAs, RAs, OCSP responders or Subscribers shall protect activation data from disclosure or compromise. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect and shall not be stored with the cryptographic module.

6.4.3 Other Aspects of Activation Data

No Stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards.

At a minimum LAWtrust data centre shall have (but not limited to) the following controls to ensure security of the systems:

- Integrity checks are performed on the operating system;
- Software packages are only installed from a trusted software repository;
- Minimal network connectivity;
- Authentication and authorization for all functions;
- Strong authentication and role-based access control for all vital functions;
- Disk and file encryption for all relevant data; and
- Proactive patch management.

6.5.2 Computer Security Rating

LAWtrust PKI CAs Software shall comply with at least Common Criteria EAL2 or an equivalent security profile from other applicable standards.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

LAWtrust utilise approved commercial products for the core PKI components.

6.6.2 Security Management Controls

The configuration of LAWtrust PKI CA systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology shall be used for installation and on-going maintenance of the system.

6.6.3 Life Cycle Security Ratings

Any of LAWtrust PKI CA IT systems or components that are replaced are taken out of operation in such a way that the functions thereof and data contained therein cannot be misused. In addition, any changes to IT systems or components are logged.

6.7 Network Security Controls

LAWtrust PKI CA shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such protection mechanisms may include network security and firewall management, port restrictions and IP address filtering. Unused services shall be turned off.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

6.8 Time Stamping

Time stamping shall be supported for the Certificates, CRLs, and other revocation database entries containing time and date information. LAWtrust PKI CA shall ensure the synchronization of CA components using a trusted time source, such as a Network Time Protocol (NTP) service or an atomic clock.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

This section contains the rules and guidelines followed by the CAs in populating X.509 certificates and CRL extensions. LAWtrust PKI CA shall use certificate profiles as described in the applicable section of the relevant LAWtrust PKI CPS document.

7.1.1 Version Numbers

LAWtrust PKI CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

LAWtrust PKI CA critical private extensions shall be interoperable in their intended community of use. Subordinate CA certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP.

7.1.3 Algorithm Object Identifiers

LAWtrust PKI CAs shall sign Certificates using any one of the following:

- **sha256WithRSAEncryption** algorithm (1.2.840.113549.1.1.11).
- **sha384WithRSAEncryption** algorithm (1.2.840.113549.1.1.12).
- **ecdsawithsha256** algorithm (1.2.840.10045.4.3.2)
- **ecdsawithsha384** algorithm (1.2.840.10045.4.3.3)
- **ecdsawithsha512** algorithm (1.2.840.10045.4.3.4)

The algorithm identifier of the subject Public Key shall be:

- **rsaEncryption (OID: = 1.2.840.113549.1.1.1).**

7.1.4 Name Forms

Certificates issued by LAWtrust PKI CA shall contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5 Name Constraints

No Stipulation.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert a certificate policy OID.

7.1.7 Usage of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No Stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension shall conform to X.509 certification path processing rules.

7.2 CRL Profile

LAWtrust PKI CA CRL Profile is as below:

Field	Content	Comment
Version	1	
Algorithm	SHA256withRSA	
Issuer	<CN= LAWtrust Root CA 2048> <CN= LAWtrust Root CA2 4096> <CN= LAWtrust AeSign CA01> <CN= LAWtrust AeSign CA02> <CN= LAWtrust AATL CA01> <CN= LAWtrust Auth CA02> <CN= LAWtrust Signing CA01> <CN= LAWtrust Auth CA01> <CN= LAWtrust Secure CA01> O=LAWtrust C=ZA	The CN attribute reflects the Common name of the CA signing the CRL, thus each CA (Root and Issuing CA) will reflect their CN attribute on the CRL they sign
This update	*<issue date>*	Date CRL was issued
Next update	*<issue date + 6 months> For Root CA* *<issue date + n days> For ICAs* *n min = 1 day* *n max = 6 days* *(Specific per CA as per CPS)*	Or immediately upon revocation
AuthorityKeyIdentifier	Parent CA's Subject Key Identifier	Key identifier of the CA signing the CRL
CRL number	<number>	Monotonically increasing number

7.2.1 Version Numbers

LAWtrust PKI CA shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.2 CRL and CRL Entry Extensions

Critical private extensions shall be interoperable in their intended community of use. CRLs shall have the CRL number and Authority Key Identify extensions set.

7.3 OCSP Profile

OCSP requests and responses shall be in accordance with RFC 6960.

7.3.1 Version Number

The version number for request and OCSP responses shall be v1.

7.3.2 OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

LAWtrust Security Committee shall be responsible for overseeing compliance of LAWtrust PKI CAs to the LAWtrust CP and applicable CPS. The LAWtrust PA shall ensure that the requirements of the LAWtrust PKI CA CP and applicable CPS are implemented and enforced.

LAWtrust Security Committee shall ensure adherence of the Issuing CAs to this CP, accompanying CPS and any applicable laws and regulations. LAWtrust Security Committee shall also ensure the Issuing CAs comply with audit requirements.

8.1 Frequency of Audit or Assessments

LAWtrust Root CAs shall be subjected to a periodic WebTrust compliance audits which are no less frequent than once a year.

The Issuing CAs shall also be audited to ensure compliance against defined requirements on at least an annual basis.

8.2 Identity and Qualifications of Assessor

The annual audit of LAWtrust PKI CA shall be performed by an Independent Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme; and
- Bound by law, government regulation, or professional code of ethics.

8.3 Assessor's Relationship to Assessed Entity

To provide an unbiased and independent evaluation, the auditor and audited party shall not fall under the same company or group of companies.

8.4 Topics Covered By Assessment

The compliance audits will verify whether LAWtrust PKI operations environment is in compliance with the applicable CP, CPS and supporting operational policies and procedures. The term LAWtrust PKI Operations environment defines the total environment and includes:

- All documentation, records;
- Contracts/agreements;
- Compliance with applicable Law;
- Physical and logical controls;
- Personnel and approved roles/tasks;
- Hardware (e.g. servers, desktops, hardware security modules, network devices and security devices); and
- Software and information.

The auditor shall provide LAWtrust PKI CA with a compliance report highlighting any discrepancies.

8.5 Actions Taken As A Result of Deficiency

If irregularities are found by the auditor, LAWtrust PKI CA shall be informed in writing of the findings. The audited party must submit a report to the auditor or directly to LAWtrust PKI as to any remedial action the audited party will take in response to the identified deficiencies. This report shall include a time for completion to be approved by the auditor.

Where LAWtrust PKI CA fails to take remedial action in response to the identified deficiencies, LAWtrust Security Committee shall be informed by the auditor and shall take the appropriate action, according to the severity of the deficiencies.

8.6 Communication of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to LAWtrust PKI PA and LAWtrust Security Committee.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fee

LAWtrust PKI CAs may charge fees for certificate issuance or renewal. Fees may also be charged for certificate reissuance or re-key.

9.1.2 Certificate Access Fees

LAWtrust PKI CAs may charge access fees at its discretion to any database which stores issued certificates.

9.1.3 Revocation or Status Information Access Fee

LAWtrust PKI does not charge fees to access certificate status information via the CRL or OCSP service.

9.1.4 Fees for Other Services

LAWtrust PKI may charge fees for other services such as timestamping.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

LAWtrust PKI disclaims all liability implicit or explicit due to the use of any certificates issued by the Issuing CAs which certify public keys of subscribers.

9.2.1 Insurance Coverage

LAWtrust PKI shall hold insurance cover in lieu of its performance and obligations that is deemed sufficient by the CA:

- Commercial general liability insurance with policy limits as determined by LAWtrust;
- Professional Liability (Errors and Omissions) Insurance with policy limits as determined by LAWtrust.

9.2.2 Other Assets

LAWtrust PKI shall have sufficient financial resources to maintain their operations and perform their duties.

9.2.3 Insurance/warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

Information pertaining to the CA and not requiring protection may be made publicly available at the discretion of LAWtrust Security Committee or LAWtrust PKI PA. Specific confidentiality requirements for business information are defined in the LAWtrust PKI Privacy Policy and the applicable Agreements.

9.3.1 Scope of Confidential Information

Any corporate or personal information held by LAWtrust PKI, LAWtrust PKI Root CAs and Issuing CAs related to the application and issuance of Certificates is considered confidential and will not be released without the prior consent of the relevant holder, unless required otherwise by law or to fulfil the requirements of this CP, and in accordance with LAWtrust PKI Privacy Policy. LAWtrust Data Classification Policy specifies which documents are considered to be confidential. Information contained in certificates and related certificate status is not confidential.

9.3.2 Information not within the Scope of Confidential Information

Such information as specified by LAWtrust PKI PA, LAWtrust PKI Privacy Policy, LAWtrust PKI Document Control Policy, LAWtrust PKI Operations Policies and procedures and applicable Agreements.

9.3.3 Responsibility to Protect Confidential Information

All LAWtrust PKI participants shall be responsible for protecting the confidential information they possess in accordance with LAWtrust PKI Privacy Policy and applicable laws and Agreements.

9.4 Privacy of Personal Information

Any personal identifying information collected by LAWtrust PKI shall be protected in accordance with LAWtrust Personnel Security Policy. LAWtrust PKI shall use reasonable measures to protect personal identifying information from disclosure to any third party.

9.4.1 Privacy Plan

All personally identifying information as defined by LAWtrust Personnel Security Policy shall be protected from unauthorized disclosure.

9.4.2 Information Treated as Private

Any information about Issuing CAs that is not publicly available through the content of the issued certificate, repository and online CRL's is treated as private.

9.4.3 Information not Deemed Private

Information appearing in Issuing CA Certificates such as the organization name, and public key will not be deemed private. LAWtrust PKI Privacy Policy identifies the personally identifiable information that can be collected to enable issuance of a certificate.

9.4.4 Responsibility to Protect Private Information

Access to LAWtrust PKI held private information shall be restricted to those with an official need-to-know basis in order to perform their official duties.

9.4.5 Notice and Consent to Use Private Information

Requirements for notice and consent to use private information are defined in the respective Agreements and LAWtrust PKI Privacy Policy.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Any disclosure shall be handled in accordance with LAWtrust PKI Privacy Policy.

9.4.7 Other Information Disclosure Circumstances

Any disclosure shall be handled in accordance with LAWtrust PKI Privacy Policy.

9.5 Intellectual Property Rights

LAWtrust PKI retains exclusive rights to any products or information developed under or pursuant to this CP.

9.6 Representations and Warranties

9.6.1 LAWtrust PKI CA's Representations and Warranties

LAWtrust PKI Root CAs provide representations and warranties in accordance with this CP, respective agreements and applicable laws and regulations as below:

- Providing the operational infrastructure and certification services;
- Making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" include but are not limited to operating in compliance with:
  - Documented CP and applicable CPS;
  - Documented LAWtrust PKI Operations Policies and Procedures
- At the time of Certificate issuance; LAWtrust PKI implemented procedure for verifying accuracy of the information contained within it before installation and first use;
- Implemented a procedure for reducing the likelihood that the information contained in the Certificate is not misleading;
- Maintaining 24x7 publicly accessible repositories with current information and replicates LAWtrust PKI issued certificates and CRLs;
- For the CA's, the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key. CA private key is generated using multi-person control "m-of-n" split key knowledge scheme;
- Backing up of the CA signing Private Key is under the same multi-person control as the original Signing Key;
- Keep confidential, any passwords, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control procedures for all such personal secrets;
- Use its private signing key only to sign certificates and CRLs and for no other purpose;
- Perform authentication and identification procedures in accordance with applicable Agreement and LAWtrust PKI Operations Policies and Procedures;
- Provide certificate and key management services in accordance with the CP and CPS; and
- Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes.

9.6.2 RA Representations and Warranties

LAWtrust PKI CA requires all RAs under its PKI Hierarchy to warrant that they are in compliance with this CP and the relevant CPS and may choose to include additional representations within its CPS or RA agreement.

9.6.3 Relying Parties Representations and Warranties

Relying Parties who rely upon the certificates issued under LAWtrust PKI shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Verify the Validity by ensuring that the Certificate has not expired;
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 amendment;
- Ensure that the Certificate has not been suspended or revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon; and
- Determining that such Certificate provides adequate assurances for its intended use.

9.6.4 Subscriber Representations and Warranties

Subscribers are human individuals or organization entities to which certificates are issued.

1. It is the responsibility of the Subscriber to:
   - Provide accurate and complete information at all times to the CA/RA, both in the certificate request and verification process defined by the CA/RA for specific Certificate type to be supplied by LAWtrust PKI;
   - Review and verify the Certificate contents for accuracy;
   - Secure private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key;
   - Use the Subscriber Certificate only for its intended uses as specified by LAWtrust PKI;
   - Notify the CA/RA in the event that any information in the Certificate is, or becomes, incorrect or inaccurate;
   - Notify the CA/RA in the event of a key compromise immediately whenever the Subscriber has reason to believe that the Subscriber's private key has been lost, accessed by another individual, or compromised in any other manner;
   - Use the Subscriber Certificate in a manner that does not violate applicable laws in the Republic of South Africa;

- Upon termination of Subscriber Agreement, revocation or expiration of the Subscriber Certificate, immediately cease use of Private Key corresponding to the Public Key included in the Subscriber Certificate.

2. Subscriber agrees that any use of the Subscriber Certificate to sign or otherwise approve the contents of any electronic record or message is attributable to Subscriber. Subscriber agrees to be legally bound by the contents of any such electronic record or message.
3. Subscriber shall indemnify and hold LAWtrust PKI or RA acting on behalf of LAWtrust PKI, harmless from and against any and all damages (including legal fees), losses, lawsuits, claims or actions arising out of:

   - Use of Subscriber's Certificate in a manner not authorized by LAWtrust PKI or otherwise inconsistent with the terms of this Subscriber Agreement or LAWtrust PKI;
   - A Subscriber Certificate being tampered with by the Subscriber; or
   - Inaccuracies or misrepresentations contained within the Application. A Subscriber shall indemnify and hold the CA/RA harmless against any damages and legal fees that arise out of lawsuits, claims or actions by third parties who rely on or otherwise use Subscriber's Certificate, where such lawsuit, claim, or action relates to a Subscriber's breach of its obligations outlined in this Subscriber Agreement or LAWtrust PKI, a Subscriber's use of or reliance upon a Subscriber Certificate in connection with its business operations, a Subscriber's failure to protect its private key, or claims pertaining to content or other information or data supplied, or required to be supplied, by Subscriber.

9.7 Disclaimers of Warranties

LAWtrust PKI, through its associated components, seeks to provide digital certification services according to international standards and best practices, using the most secure physical and electronic installations.

LAWtrust PKI provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of LAWtrust PKI or for the legal validity, acceptance or any other type of recognition of its own certificates, those issued by it through its Subordinate Issuing CA's, any digital signature backed by such certificates, and any products provided by LAWtrust PKI. LAWtrust PKI further disclaims any warranty of merchantability or fitness for a particular purpose of the above-mentioned certificates, digital signatures and products.

9.8 Limitations of Liability

Limitations on Liability:

- LAWtrust PKI will not incur any liability to any person to the extent that such liability results from their negligence, fraud or willful misconduct;

- LAWtrust PKI assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under Certificate Policy for any use other than in accordance with Certificate Policy. Relying Parties will immediately indemnify LAWtrust PKI from and against any such liability and costs and claims arising there from;
- LAWtrust PKI will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services;
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations described in the Relying Party agreement;
- LAWtrust PKI denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

9.9 Indemnities

Notwithstanding any limitations on its liability to its Sub-CAs and Relying Parties, LAWtrust PKI understands and acknowledges that the Application Software Suppliers who have supplied the CA software in use by LAWtrust PKI do not assume any obligation or potential liability of LAWtrust PKI under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, LAWtrust PKI SHALL defend, indemnify and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved.

LAWtrust PKI shall indemnify, defend and hold harmless the following parties:

- Its directors, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorney's fees), judgments, awards or liability;
- Any parties relying on LAWtrust PKI certificates or arising as a result of an infringement or violation of any patents, copyrights, trade secrets, licenses, or other property rights of any third party.

9.10 Term and Termination

9.10.1 Term

This CP shall be effective upon approval by the LAWtrust Security Committee. Once the CP becomes effective it is published in the repository. Amendments to this CP upon approval become effective and replace the older version in the repository.

9.10.2 Termination

This CP, as amended from time to time, shall remain in force until it is replaced by a new version. The latest version of LAWtrust CP can be found at the LAWtrust PKI Repository.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, all LAWtrust PKI participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

All communication between LAWtrust PKI CA and LAWtrust PA shall be in writing or via digitally signed communication. If in writing, the communication shall be signed on the appropriate organization letterhead. If electronically, a Digital Signature shall be made using a Private Key whose companion Public Key is certified using a Certificate meeting this CP's Certificate assurance level.

9.12 Amendments

9.12.1 Procedure for Amendment

LAWtrust PKI PA shall review this CP at least once per year. Errors, updates, or suggested changes to this CP shall be communicated to LAWtrust. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change. Any technical changes in the LAWtrust PKI Infrastructure shall be managed as per the LAWtrust PKI Change Management Policy.

LAWtrust PKI reserves the right to change this CP from time to time. LAWtrust PKI will incorporate any such change into a new version of this CP and, upon approval, publish the new version. The new CP will carry a new version number.

9.12.2 Notification Mechanism and Period

This CP and any subsequent changes shall be made available to the LAWtrust PKI participants within two weeks of approval. LAWtrust PKI reserves the right to amend this CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL's, and changes to contact information. All LAWtrust PKI participants and other parties designated by LAWtrust PKI shall provide their comments to LAWtrust PKI in accordance with its rules. LAWtrust PKI's decision to designate amendments as material or non-material shall be at LAWtrust PKI's sole discretion.

9.12.3 Circumstances under which OID must be changed

The policy OID shall only change if the change in the CP results in a material change to the trust by the relying parties, as determined by LAWtrust PKI.

9.13 Dispute Resolution Procedures

The use of certificates issued by LAWtrust PKI is governed by contracts, agreements, and standards set forth by LAWtrust PKI. Those contracts, agreements and standards include dispute resolution policy and procedures that shall be employed in any dispute arising from the issuance or use of a certificate governed by this CP. Dispute Resolution mechanism is described in LAWtrust PKI Dispute Resolution Policy.

9.14 Governing Law

This CP is governed by the laws of the Republic of South Africa.

9.15 Compliance with Applicable Law

This CP is subject to applicable national, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of LAWtrust PKI PA.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

This document shall be treated according to laws of the Republic of South Africa. Legal disputes arising from the operation of LAWtrust PKI CA will be treated according to the laws of the Republic of South Africa.

9.16.5 Force Majeure

LAWtrust PKI CA shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and reasons beyond provisions of the governing law.

9.17 Other Provisions

9.17.1 Fiduciary Relationships

Nothing contained in this CP shall be deemed to constitute either LAWtrust PKI, or any of its subcontractors, agents, officers, suppliers, employees, partners, principals, or directors to be a partner, Affiliate, trustee, of any Relying Party or any third party, or to create any fiduciary relationship between LAWtrust PKI CA and any Relying party, or any third party, for any purpose whatsoever.

Nothing in this CP or any Agreement between a third party and a Relying Party shall confer on any Customer, Relying Party, Applicant or any third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the LAWtrust PKI CA.

9.17.2 Administrative Processes

Administrative process shall be specified in corresponding agreements and any LAWtrust PKI Operations Policies.

10. APPENDIX A (DEFINITIONS)

Term	Definition
Applicant	An entity making an application for a digital certificate.
Asymmetric cryptography	Asymmetric cryptography or public Key cryptography is cryptography in which a pair of keys issued to a subscriber and the keys are used to encrypt and or decrypt messages to achieve authenticity and confidentiality. An applicant applies for a digital certificate, if successful a key pair is generated and a certificate signing request is sent to a certificate Authority which then signs the public key and returns a public key certificate to the applicant. The public key and its corresponding private key are uniquely linked mathematically.
Audit Trail Files	Secured audit log/trail files are stored on the CA server and can only be viewed by authorised personnel logged into the administration interface.
Authentication	Authentication is a mechanism to validate the identity of a user and or a computing device requesting permission to access computing resources or technology services supporting business processes.
Authentication factors	A factor of authentication refers to a mechanism used to facilitate the authentication of a user or devices requesting access to computing resources. The following factors of authentication are universally accepted; Location of the computing interface(controlled access and managed), Something the requester has(Possession of something which is validated), Something the requester knows(secret password or PIN), Something the requester is(biometrics)
Authentication scheme	Industry accepted authentication schemes include one or more factors of authentication. The choice of authentication factors and the process behind establishing credentials within each factors within the chosen scheme determine the strength of the authentication.
CA	See definition of certificate/certification authority.
Certificate Administrator	A trusted individual that performs certain trusted tasks (e.g. authentication) on behalf of a CA or RA. This person is usually a member of the personnel of such CA or RA.
Certificate	See definition of digital certificate.
Certificate/Certification Authority	A legal entity that issues, signs, manages, revokes and renews digital certificates.
Certificate Policy	A named set of rules that indicate the applicability of a digital certificate to a particular community and or class of application with common security requirements. The practices required to give effect to the rules set out in the certificate policy are set out in the certification practice statement.
Certification Practice Statement	In order to comply with the rules set out in the certificate policy, the CPS details the practices that a certificate authority needs to employ when issuing, managing, revoking, renewing, and providing access to digital certificates, and further includes the terms and conditions under which the certificate authority makes such services available.
CP	See definition of certificate policy.
CPS	See definition of certification practice statement.
Chained	A Certificate Chain linking the chain of trust from the highest level of trust, that being the Root CA, any subordinate CA's and or Issuing CA's.

Term	Definition
Cryptography	Cryptography is about message secrecy, and is a main component in information security and related issues, particularly, authentication, and access control. One of cryptography's primary purposes is hiding the meaning of messages, not usually the existence of such messages.
Cryptography Services	A service provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of a digital certificate/digital signature scheme for the purpose of ensuring (i) that data or data messages can be accessed or can be put into an intelligible form only by certain persons, (ii) that the authenticity or integrity of such data or data message is capable of being ascertained, (iii) the integrity of the data or data message, or (iv) that the source of the data or data message can be correctly ascertained.
Data	Electronic representations of information in any form.
Data Message	Data generated, sent, received or stored by electronic means.
Digital Certificate	A digitally-signed data message that is a public-key certificate in the version 3 format specified by ITU-T Recommendation X.509, which includes the following information: (i) identity of the Certificate Authority issuing it; (ii) the name or identity of its subscriber, or a device or electronic agent under the control of the subscriber; (iii) a Public Key that corresponds to a Private Key under the control of the subscriber; (iv) the validity period; (v) the Digital Signature created using a private Key of the certificate authority issuing it; and (vi) a serial number.
Digital Signature	A transformation of a data message using an asymmetric cryptosystem such that a person having the initial data message and the signer's public key can determine whether: (i) the transformation was created using the private key that corresponds to the subscriber's public key; and (ii) the message has been altered since the transformation was made.
Digital Signature Validation	In conjunction with the public key component of the correct public/private key pair, the signature of a data object can be verified by: 1. decrypting the signature object with the public key component to expose the original hash value, 2. re-computing a hash value over the data object, and 3. Comparing the exposed hash value to the re-computed hash value. If the two values are equal the signature is often considered valid.
Digitally Sign	The act of generating a digital signature for a data message, which is created by: 1. Hashing the object to be signed with a one-way hash function; and 2. Encrypting (signing) the hash value with the private key component of a key pair. The hash value is encrypted instead of the data itself because the encryption function is typically very slow compared to the time it takes to complete the hash of the data. The object created by these two steps is called the signature and is bound to the data message according to an application specific mechanism.
ECT Act 2002	See definition of Electronic Communications and Transaction Act 2002
Electronic Communication	Communication by means of data messages.
Electronic Communication and Transactions Act, No. 25 of 2002	South African Legislation that provides for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy; to promote universal access to electronic communications and transactions and the use of electronic transactions by businesses.
Email	Electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication.

Term	Definition
Identity Document	An identity document is used to verify aspects of a person's identity. Recognized identity documents for natural persons are; 1. For South African citizens applying from within or outside of the South African Border; a. The applicant should be a current and valid citizen of South Africa. (Presence of ID document is sufficient) b. A valid and original "Green" Identity document or National ID Card issued by the South African Department of Home Affairs c. A valid and original Passport issued by the South African Department of Home Affairs d. A valid and original temporary identity document issued by the South African Department of Home Affairs. 2. For non-South African Nationals, applying from any location outside of the applicant's stated country of citizenship. a. The applicant should be a current and valid citizen of stated country of citizenship. (Presence of ID document is sufficient) b. Passport issued by the applicant's stated country of citizenship's, authorized government body responsible for issuing passports to citizens of the stated country, or c. identity document issued from the authorized government body responsible for issuing identity documents to citizens of the stated country. d. Any photo ID, which contains the Applicant's full names and surname and which is recognised as a valid form of identification by the country or state of issue
integrity	Integrity is a cryptography service that ensures that modifications to data are detectable.
key pair	Two mathematically related cryptographic keys, referred to as a private key and a public key, having the properties that (i) one key (the public key) can encrypt a message which only the other key (the private key) can decrypt, and (ii) even knowing the one key (the public key), it is computationally infeasible to discover the other key (the private key).
LAWtrust Root CA	See also the definition of certification authority. The Root certification authorities managed by LAWtrust including the LAWtrust Root Certification Authority 2048 and the LAWtrust Root Certification Authority 2 (4096)
LAWtrust Subordinate CA Certificate	See definition of digital certificate. All digital certificates issued by a LAWtrust Subordinate.

Term	Definition
LAWtrust OA	LAWtrust Management forum responsible for the implementation of the LAWtrust Policy and Practices and the Operations of the LAWtrust PKI environment
LAWtrust PA	LAWtrust Management forum responsible for defining the LAWtrust Policy and Practices and ensuring that the Policies and Practices are adhered to.
LDAP	A software protocol for enabling anyone to locate organisations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
Master Services Agreement	The contract between LAWtrust and an appointed registration authority stipulating the terms and conditions for the registration authority to manage certificate lifecycle activities on behalf of the LAWtrust Root CA.
MSA	Master Services Agreement,
Non-Repudiation	The ability to prevent a party from refusing to fulfil an obligation or denying the truth or validity of an electronic communication facilitated by appropriate use of the LAWtrust Services.
OCSP	Online Certificate Status Protocol is an Internet protocol, employed to ascertain the revocation status of an X.509 digital certificate. An alternative to CRL based checking.
OCSP Responder	An online service hosted by Lawtrust and connected to Lawtrust repositories in order to process OCSP certificate revocation checks.
Private Key	The key of a key pair used to create a digital signature and is required to be kept secret.
Public Key	The key of a Key Pair used to verify a Digital Signature and may be publicly disclosed.
Public Key Cryptography	Public key cryptography is about using mathematically related keys, a public key and a private key, in order to implement a digital certificate /digital signature scheme, also known as an asymmetric crypto system.
PKI	See definition of public key infrastructure.
Public Key Infrastructure	The structure of hardware, software, people, processes and policies that collectively support the implementation and operation of a certificate-based public key cryptography scheme.
RA	See definition of registration authority.
RA-Agent	An person that is acting on behalf of the LAWTrust Registration Authority and who was authorised by LAWtrust to act as RA agent on behalf of the LAWtrust RA.
Registration Authority	An entity that: (i) receives certificate applications, and (ii) validates information supplied in support of a certificate application, (iii) requests a certificate authority to issue a certificate containing the information as validated by the registration authority, and (iv) requests a certificate authority to revoke certificates issued;
Relying Party	A person that relies on a certificate or other data that has been digitally signed.
Relying Party Agreement	An agreement between the certificate authority and a relying party that sets out the terms and conditions governing reliance upon a certificate or data that has been digitally signed

Term	Definition
Signature	Any mark made by a person that evidence's that person's intention to bind himself/herself to the contents of a document to which that mark has been appended. Depending on the circumstances, this could be a handwritten signature or a digital signature.
Subscriber	An applicant whose Certificate Application has been approved, and has been issued a certificate, and who is the subject named or otherwise identified in the certificate, controls the private key that corresponds to the public key listed in that certificate, and is the individual to whom digitally signed data messages verified by reference to such certificate are to be attributed.
Subscriber Agreement	An agreement between the certificate authority and a subscriber that sets out the terms and conditions governing the issuance of a certificate, control of the private key that corresponds to the public key listed in the certificate, acceptable use of the certificate, notification of compromise of the private key, and matters ancillary and related thereto.
Verification	Verification is the act of checking that information is accurate. It is used in the following manor a) At registration, the act of evaluating the subscribers' credentials as evidence for their claimed identity; b) During use, the act of comparing electronically submitted identity and credentials with stored values to prove identity. c) Relying Party will check the certificates used as per the relying Party Agreement.

11. SIGN OFF ACCEPTANCE

Name:	Marcile De Waal
Authority:	Policy Authority
Title:	Senior Specialist: Policy Authority and Assurance
Date:	2026-10-16
Signature:	